(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 976 199 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
01.10.2008 Bulletin 2008/40

(21) Application number: **06832409.4**

(22) Date of filing: **01.11.2006**

(51) Int Cl.:
H04L 12/56 *(2006.01)* ***H04L 9/32*** *(2006.01)*
H04L 12/22 *(2006.01)* ***H04M 3/00*** *(2006.01)*
H04Q 7/38 *(2006.01)*

(86) International application number:
PCT/JP2006/321893

(87) International publication number:
WO 2007/052713 (10.05.2007 Gazette 2007/19)

(84) Designated Contracting States:
DE GB

(30) Priority: **01.11.2005 JP 2005318917**

(71) Applicant: **NTT DoCoMo, Inc.**
Chiyoda-ku
Tokyo 100-6150 (JP)

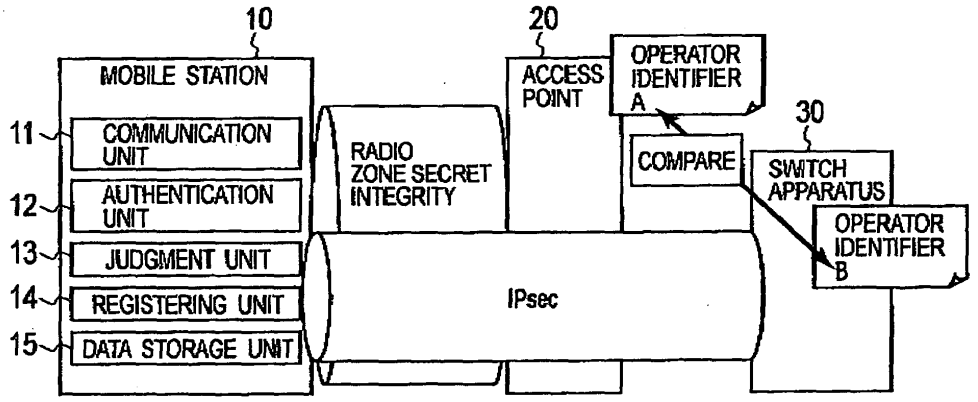
(72) Inventors:
- **TAHARA, Takuhisa**
  Intellectual Property Dept.
  Chiyoda-ku, Tokyo 100-6150 (JP)
- **TANABE, Akimichi**
  Intellectual Property Dept.
  Chiyoda-ku, Tokyo 100-6150 (JP)
- **NOGUCHI, Katsuhiro**
  Intellectual Property Dept.
  Chiyoda-ku, Tokyo 100-6150 (JP)
- **KAWAKATSU, Shinpei**
  Intellectual Property Dept.
  Chiyoda-ku, Tokyo 100-6150 (JP)

(74) Representative: **HOFFMANN EITLE**
Patent- und Rechtsanwälte
Arabellastrasse 4
81925 München (DE)

(54) COMMUNICATION SYSTEM, MOBILE STATION, SWITCHING MACHINE AND COMMUNICATION METHOD

(57) A communication system according to the present invention includes: a mobile station 10; an access point located on a radio access system; and a switch apparatus 30 connected to the radio access system, wherein a secured connection between a mobile station 10 and the access point 20 has been already established. The mobile station 10 includes a judgment unit 30 configured to judge whether or not to establish a secured connection between the mobile station 10 and the switch apparatus 30.

FIG. 1



EP 1 976 199 A1

Description

[Technical Field]

[0001] The present invention relates to a communication system, a mobile station, a switch apparatus, and a communication method, which establish a secured connection.

[Prior Art]

[0002] As for a radio network system, an IMS (Internet Protocol Multimedia Subsystem) has drawn attention in recent years. The IMS is a standard for converting services which have been provided so far through fixed networks, mobile communications, broadcasting, and the like into IP-based services so that a fused multimedia service is achieved.

[0003] The IMS is designed as an infrastructure completely independent of an access network so that it can be managed by a business owner other than a mobile operator. A secure communication is achieved by providing an encryption function between a mobile station and an IMS apparatus. For example, as shown in Fig. 20, when a connection ensuring a secret/an integrity is established between a mobile station 10 and an access point 20 located on a radio access system, a secure connection is further established between the mobile station 10 and a switch apparatus 30 (here, an IMS apparatus) connected to the radio access system.

[0004] A procedure for establishing such a connection is described with reference to Fig. 21 (for example, refer to Non-Patent Document 1). Note that, Fig. 21 is a procedure in accordance with the 3GPP.

[0005] First, the mobile station 10 performs an authentication with the access point 20 located on the radio access system so as to exchange a secret key and an integrity key (S901). Then, the mobile station 10 stores an algorithm for the secret and the Integrity to be used in a radio zone (S902). Here, a secure connection is established between the mobile station 10 and the access point 20, located on the radio access system.

[0006] Next, the mobile station 10 transmits a user ID, an authentication request, an IPsec security association, and the like to the switch apparatus 30 (here, a P-CSCF (Proxy Call Session Control Function) 30a) so as to perform a SIP registration (S903). Next, the P-CSCF 30a transmits the user ID, the authentication request, and the like to a S-CSCF (Serving Call Session Control Function) 30b so as to perform the SIP registration (S904), and the S-CSCF 30b transmits a random number, the secret key, the integrity key, and the like to the P-CSCF 30a so as to perform an authentication challenge (S905). Next, the P-CSCF stores the secret key and the integrity key (S906). Next, the P-CSCF 30a transmits the random number, the secret key, the integrity key, and the like to the mobile station 10 so as to perform the authentication challenge (S907). Here, the secured connection is established between the access point 20 located on the radio access system and the switch apparatus 30

[0007] Thereafter, the mobile station 10 transmits the user ID, a challenge response, an IPsec used algorithm, and the like to the P-CSCF 30a so as to perform the SIP registration (S908), and the P-CSCF 30a transmits the user ID, the challenge response, a validity of an IPsec secret and the Integrity, and the like, to the S-CSCF 30b so as to perform the SIP registration (S909). Next, the S-CSCF 30b transmits to the P-CSCF 30a the validity of the authentication (S910), and the P-CSCF 30a transmits to the mobile station 10 the validity of the authentication (S911).

[0008] However, it is common that a mobile operator has already ensured a security between the mobile station and the radio access system by applying an encryption to the radio access network, and it is also common that the mobile operator physically ensures a security for a zone from the radio access system to the IMS apparatus. Therefore, when the radio access system and the IMS apparatus accessing thereto are operated by the same operator, an encryption function of the IMS apparatus becomes redundant.

[0009] Further, for a future radio network system, based on the IMS, various services such as a VoIP and a Push to Talk are assumed to be achieved. Accordingly, shortening a time of a connection delay in connecting to the IMS apparatus, and reducing a process load on the mobile station and the network are important factors for improving a quality of a service and using the resources effectively.

Non-Patent Document 1: 3GPP TS33.203 V6.8.0

[Disclosure of the Invention]

[0010] Therefore, the present invention was made in view of the above-mentioned problems, and an object thereof is to provide a communication system, a mobile station, a switch apparatus, and a communication method, which can shorten a time of delay in connecting the mobile station and a network, and reduce a process load on the mobile station and the network.

[0011] In order to solve the above problem, a first aspect of the present invention is summarized as a communication system for establishing a secured first connection between a mobile station and an access point located on a radio access system, including: a judgment unit configured to judge whether or not to establish secured second connection between the mobile station and a switch apparatus connected to the radio access system.

[0012] In the first aspect of the present invention, the judgment unit may judge where or not to establish the secured second connection, by comparing an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which is received from the switch apparatus and which uniquely identifies an appa-

ratus controlling the switch apparatus.

[0013] In the first aspect of the present invention, the communication system may further include an identifier list storage unit configured to store an identifier list which is combination of an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which uniquely identifies an apparatus controlling the switch apparatus. And the judgment unit may be configured to judge whether or not to establish the secured second connection by comparing the identifier list, with the identifier which is received from the access point and which uniquely identifies the apparatus controlling the radio access system, and the identifier which is received from the switch apparatus and which uniquely identifies the apparatus controlling the switch apparatus.

[0014] In the first aspect of the present invention, the communication system may further include an identifier storage unit configured to store an identifier which uniquely identifies an apparatus controlling the switch apparatus, and the judgment unit may be configured to judge whether or not to establish the secured second connection, by comparing an identifier which is stored in the identifier storage unit, and an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system.

[0015] In the first aspect of the present invention, the communication system may further include an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system or a non-secured algorithm used in the radio access system, and the judgment unit may be configured to judge whether or not to establish the secured second connection by comparing an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which is received from the switch apparatus and which uniquely identifies an apparatus controlling the switch apparatus, and by comparing the algorithm list and the algorithm used in the radio access system.

[0016] In the first aspect of the present invention, the communication system may further includes: an identifier list storage unit configured to store an identifier list which is a combination of an identifier which is received from the access point and which uniquely identifies an apparatus controlling the switch apparatus, and an identifier which uniquely identifies an apparatus controlling the the switch apparatus; and an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system and a non-secured algorithm used in the radio access system, and the judgment unit may be configured to judge whether or not to establish the secured second connection, by comparing an identifier which is received from the access point and which uniquely identifies an apparatus controlling the switch apparatus, and by comparing the algorithm list and the algorithm used in the radio access system.

[0017] In the first aspect of the present invention, the communication system may further include, in the mobile station: an identifier storage unit configured to store an identifier which uniquely identifies an apparatus controlling the switch apparatus; and an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system and a non-secured algorithm used in the radio access system, and the judgment unit may be configured to judge whether or not to establish the secured second connection, by comparing an identifier which is stored in the identifier storage unit, and an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and by comparing the algorithm list and the algorithm used in the radio access system.

[0018] In the first aspect of the present invention, the communication system may further include an address list storage unit configured to store an address list which indicates a range of an address assigned by the radio access system on which the switch apparatus is located, and the judgment unit may be configured to judge whether or not to establish the secured second connection, by comparing the address list and an address of the mobile station which is transmitted from the mobile station.

[0019] In the first aspect of the present invention, the communication system may further include: an address list storage unit configured to store an address list which indicates a range of an address assigned by the radio access system on which the switch apparatus is located; and an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system or a non-secured algorithm used in the radio access system on which the access point is located, and the judgment unit may be configured to judge whether or not to establish the secured connection, by comparing the address list and an address of the mobile station which is transmitted from the mobile station, and by comparing the algorithm list and the algorithm used in the radio access system on which the access point is located.

[0020] A second aspect of the present invention is summarized as a mobile station for establishing a secured first connection with an access point located on a radio access system, including: a judgment unit configured to judge whether or not to establish a secured second connection between the mobile station and a switch apparatus connected to the radio access system.

[0021] A third aspect oft the present invention is summarized as a switch apparatus connected to a radio access system in a communication system for establishing a secured first connection between a mobile station and an access point located on the radio access system, including: a judgment unit configured to judge whether or not to establish a secured second connection between the mobile station and the switch apparatus.

[0022] A fourth aspect of the present invention is summarized as a communication method in a communication system provided with a mobile station, an access point

located on a radio access system, and a switch apparatus connected to the radio access system, including: establishing a first secured connection between the mobile station and the access point; and determining whether or not to establish a secured second connection between the mobile station and the switch apparatus.

[Brief Descriptions of the Drawings]

[0023]

[Fig. 1] Fig. 1 is a diagram showing a configuration of a communication system according to a first embodiment of the present invention.
[Fig. 2] Fig. 2 is a sequence diagram showing a communication method according to the first embodiment of the present invention.
[Fig. 3] Fig. 3 is a diagram showing a configuration of a communication system according to a second embodiment of the present invention.
[Fig. 4] Fig. 4 is an example of an operator identifier list according to the second embodiment of the present invention.
[Fig. 5] Fig. 5 is a sequence diagram showing a communication method according to the second embodiment of the present invention.
[Fig. 6] Fig. 6 is a diagram showing a configuration of a communication system according to a third embodiment of the present invention.
[Fig. 7] Fig. 7 is a sequence diagram showing a communication method according to the third embodiment of the present invention.
[Fig. 8] Fig. 8 is a diagram showing a configuration of a communication system according to a fourth embodiment of the present invention.
[Fig. 9] Fig. 9 is an example or a radio zone algorithm list according to the fourth embodiment of the present invention.
[Fig.10] Fig. 10 is a sequence diagram showing a communication method according to the fourth embodiment of the present invention.
[Fig. 11] Fig. 11 is a diagram showing a configuration of a communication system according to a fifth embodiment of the present invention.
[Fig. 12] Fig. 12 is a sequence diagram showing a communication method according to the fifth embodiment of the present invention.
[Fig. 13] Fig. 13 is a diagram showing a configuration of a communication system according to a sixth embodiment of the present invention.
[Fig. 14] Fig. 14 is a sequence diagram showing a communication method according to the sixth embodiment of the present invention.
[Fig. 15] Fig. 15 is a diagram showing a configuration of a communication system according to a seventh embodiment of the present invention.
[Fig. 16] Fig. 16 is an example of IP address list according to the seven embodiment of the present invention.
[Fig. 17] Fig. 17 is a sequence diagram showing a communication method according to the seventh embodiment of the present invention.
[Fig. 18] Fig. 18 is a diagram showing a configuration of a communication system according to an eighth embodiment of the present invention
[Fig. 19] Fig. 19 is a sequence diagram showing a communication method according to the eighth embodiment of the present invention.
[Fig. 20] Fig. 20 is a diagram showing a configuration of a conventional communication system.
[Fig. 21] Fig. 21 is a sequence diagram showing a communication method of a conventional communication system.

[Best Modes for carrying out the Invention]

[0024] Next, embodiments of the present invention are described with reference to the accompanying drawings. In the following descriptions of the drawings, the same or similar elements are denoted by the same or similar reference numerals, However, it should be noted that the drawings are schematic.

[0025] In the embodiments of the present invention, the following description is given for an example in which a mobile station or a switch apparatus (an IMS apparatus) detects that a security is already ensured for a communication path between the mobile station and the switch apparatus, and skips an encryption process of the IMS.

<First Embodiment>

[0026] In a first embodiment, the following description is given for an example in which the mobile station detects that an operator apparatus of a radio access system that the mobile station uses, and an operator apparatus of an IMS apparatus are the same.

(Communication System)

[0027] As shown in Fig. 1, a communication system in accordance with this embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0028] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling the radio access system. Further, the switch apparatus 30 stores an identifier (e.g., an operator identifier B) which uniquely identifies an apparatus controlling a switch apparatus.

[0029] As shown in Fig. 1, the mobile station includes a communication unit 11, an authentication unit 12, a

judgment unit 13, a registering unit 14, and a data storage unit15.

[0030] The communication unit 11 performs a communication with the access point 20 and the switch apparatus 30, and performs a transmission/reception of a secret key and a signal of various kinds.

[0031] The authentication unit 12 performs an authentication between the mobile station 10 and the access point 20, and an authentication between the mobile station 10 and the switch apparatus 30.

[0032] The judgment unit 13 judges whether or not to establish a secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 13 judges whether or not to establish the connection by comparing the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system and the identifier (e.g., the operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus.

[0033] The registering unit 14 performs a SIP registration on the switch apparatus 30.

[0034] The data storage unit 15 stores the secret key, the Integrity key, the operator identifier, data in the middle of a transmission, and the like, which are received.

(Communication Method)

[0035] Next, a communication method in accordance with the first embodiment is described with reference to Fig. 2.

[0036] First, the access point 20 stores the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S101), and the switch apparatus 30 (e.g., a P-CSCF 30a) stores the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus (S102).

[0037] Next, the mobile station 10 performs the authentication with the access point 20 located on the radio access system, so as to exchange the secret key and the integrity key (S103). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0038] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in a radio zone (S104). Here, the secured connection is established between the mobile station 10 and the access point 20 located on the radio access system.

[0039] Subsequently, the mobile station 10 transmits an operator identifier request to the P-CSCF 30a (S105), and the P-CSCF 30a transmits an operator identifier response, including the operator identifier B, to the mobile station 10 (S106). Thereafter, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the operator identifier A and the operator identifier B (S107). Here, when the operator identifier A and the operator identifier B are the same, the mobile station 10 judges that the apparatus controlling the radio access system, and the switch apparatus 30 are the same. Thus, the mobile station 10 judges that establishing the secured connection between the mobile station 10 and the switch apparatus 30 is unnecessary. Incidentally, the following processes described herein below are performed when the connection is unnecessary. When the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0040] Further, the mobile station 10 transmits a user ID, an authentication request, an IPsec unnecessary notification, and the like to the P-CSCF 30a so as to perform the SIP registration (S108), Next, the P-CSCF 30a transmits the user ID, the authentication request, and the like to the S-CSCF 30b so as to perform the SIP registration (S109), and the S-CSCF 30b transmits a random number, a secret key, an integrity key, and the like to the P-CSCF 30a so as to perform an authentication challenge (S110). Subsequently, the P-CSCF 30a stores the secret key and the integrity key (S111).

[0041] Next, the P-CSCF 30a transmits the random number, an IPsec unnecessary reception response, and the like to the mobile station 10 so as to perform the authentication challenge (S112). Thereafter, the mobile station 10 transmits the user ID, a challenge response, and the like to the P-CSCF 30a so as to perform the SIP registration (S113), and the P-CSCF 30a transmits the user ID, the challenge response, and the validity of the IPsec secret and the integrity to the S-CSCF 30b so as to perform the SIP registration (S114). Next, the S-CSCF 30b transmits the validity of the authentication to the P-CSCF 30a (S115), and the P-CSCF 30a transmits the validity of the authentication to the mobile station 10.

(Operation and effects)

[0042] In accordance with the communication system, the mobile station 10, and the communication method according to the first embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30, by comparing the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system and the identifier (e.g., the operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus. When the operator identifier A and the operator identifier B are the same, the secured connection is already established between the access point 20 located on the radio access system and the switch apparatus 30. Accordingly, the mobile station 10 judges that establishing a new connection Is unnecessary.

[0043] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the first embodiment, it is possible to skip an encryption process of the IMS and to

eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

<Second Embodiment>

[0044] In the first embodiment, the mobile station 10 compares the operator identifier stored by the access point 20 and the operator identifier stored by the switch apparatus 30; however, in a second embodiment, a description is given for an example in which a comparison Is made using an operator identifier list stored by the mobile station 10 and, thereby, the mobile station 10 judges whether or not to establish a connection.

(Communication System)

[0045] As shown in Fig. 3, a communication system according to the second embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0046] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling a radio access system. Further, the switch apparatus 30 stores an identifier (e.g., an operator identifier B) which uniquely identifiers an apparatus controlling the switch apparatus.

[0047] As shown in Fig. 3, the mobile station 10 includes a communication unit 11, an authentication unit 12, a judgment unit 13, a registering unit 14, a data storage unit 15, and an identifier list storage unit 16.

[0048] The identifier list storage unit 16 stores an identifier list being a combination of the identifier which uniquely identifies the apparatus controlling the radio access system (access point 20), in which a security is ensured or not ensured, and the identifier which uniquely identifies the apparatus controlling the switch apparatus 30. Here, "the security is ensured" means that apparatuses (the access point 20, the switch apparatus 30) making a communication, and a transmission path connecting the both apparatuses are physically secured.

[0049] As shown in Fig. 4, the operator identifier list can be set that the security is ensured even when the operator identifier (e.g., an operator Y) of the radio access system (the access point 20) and the operator identifier (e.g., an operator X) of the switch apparatus 30 are not the same, and that a new security connection (IPsec) is unnecessary.

[0050] The judgment unit 13 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. More specifically, the judgment unit 13 judges whether or not to establish the connection by comparing the identifier list with the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus 30.

[0051] The communication unit 11, the authentication unit 12, the registering unit 14, and the data storage unit 15 are the same as those of the first embodiment, so that further description thereof is omitted herein.

(Communication Method)

[0052] Next, a communication method according to the second embodiment is described with reference to Fig. 5.

[0053] First, the mobile station 10 stores the operator identifier list (S201); the access point 20 stores the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S202); and the switch apparatus 30 (e.g., an P-CSCF 30a) stores the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus (S203).

[0054] Next, the mobile station 10 performs an authentication with the access point 20 located on the radio access system, so as to exchange the secret key and the integrity key (S204). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0055] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in a radio zone (S205). Here, the secured connection is established between the mobile station 10, and the access point 20 located on the radio access system.

[0056] Next, the mobile station 10 transmits an operator identifier request to the P-CSCF 30a (S206), and the P-CSCF 30a transmits an operator identifier response, including the operator identifier B, to the mobile station 10 (S207). Thereafter, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the identifier list with the operator identifier A and the operator identifier B (S208). Here, for example, the mobile station 10 refers to the identifier list shown in Fig. 4. When the operator identifier A is "operator Y" and when the operator identifier B is "operator X", the mobile station 10 judges that the security is ensured so that a new security connection (IPsec) is unnecessary. Incidentally, the processes described herein below are performed when it is Judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0057] Meanwhile, processes of steps S209 to S217 are the same as those of steps S108 to S116 shown in Fig. 2, so that further description thereof is omitted.

(Operation and effects)

[0058] In accordance with the communication system, the mobile station 10, and the communication method according to the second embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the operator identifier list with the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system and the identifier (e.g., the operator identifier B) which uniquely identifies an apparatus controlling a switch apparatus (e.g., refer to Fig. 4).

[0059] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the second embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0060] Further, in the second embodiment, it is possible to arbitrarily rewrite the operator identifier list, and to flexibly judge whether an establishment of a connection is existed.

<Third Embodiment>

[0061] In the first embodiment, the mobile station 10 compares the operator identifier stored by the access point 20 and the operator identifier stored by the switch apparatus 30; however, in a third embodiment, a description is given for an example in which the mobile station 10 stores an identifier which uniquely identifies an apparatus controlling the switch apparatus 30, and compares this identifier with an operator identifier stored by the access point 20, and thereby, the mobile station 10 judges whether or not to establish a connection.

(Communication System)

[0062] As shown in Fig. 6, a communication system in accordance with the third embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0063] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling the radio access system.

[0064] As shown in Fig. 6, the mobile station 10 includes a communication unit 11, an authentication unit 12, a judgment unit 13, a registering unit 14, a data storage unit 15, and an identifier storage unit 17.

[0065] The identifier storage unit 17 stores the identifier (e.g., an operator identifier C) which uniquely identifies the apparatus controlling the switch apparatus 30.

[0066] The judgment unit 13 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 13 judges whether or not to establish the connection by comparing the identifier (e.g., an operator identifier C) stored by the identifier storage unit 17 and the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system.

[0067] The communication unit 11, the authentication unit 12, the registering unit 14, and the data storage unit 15 are the same as those of the first embodiment, so that further description thereof is herein omitted.

(Communication Method)

[0068] Next, a communication method in accordance with the third embodiment is described with reference to Fig. 7.

[0069] First, the mobile station 10 stores the identifier (e.g., the operator identifier C) which uniquely identifies the apparatus controlling the switch apparatus 30 (S301), and the access point 20 stores the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S302).

[0070] Next, the mobile station 10 performs an authentication with the access point 20 located on the radio access system, so as to exchange a secret key and an integrity key (S303). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0071] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in a radio zone (S304). Here, the secured connection is established between the mobile station 10, and the access point 20 located on the radio access system.

[0072] Subsequently, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the operator identifier C and the operator identifier A (S305). Here, when the operator identifier C and the operator identifier A are the same, the mobile station 10 judges that the apparatus controlling the radio access system, and the apparatus controlling the switch apparatus 30 are the same, so that the mobile station 10 judges that establishing the secured connection is unnecessary. Incidentally, the processes described herein below are performed when it is judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0073] Meanwhile, processes of steps S306 to S314 are the same as those of steps S108 to S116 shown in Fig. 2, so that further description thereof is omitted.

(Operation and effects)

[0074] In accordance with the communication system, the mobile station 10, and the communication method according to the third embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the identifier (e.g., the operator identifier C) which uniquely identifies the apparatus controlling the switch apparatus stored in the mobile station and the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system.

[0075] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the third embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0076] Further, in comparison with the first embodiment, in the third embodiment, it is unnecessary to receive the operator identifier from the switch apparatus 30, so it is possible to shorten the time of the connection delay and reduce the process load on the mobile station and the switch apparatus, even more.

<Fourth Embodiment>

[0077] In the first embodiment, the mobile station 10 compares the operator identifier stored by the access point 20 and the operator identifier stored by the switch apparatus 30; however, in a fourth embodiment, a description is given for an example in which, in addition to the above comparison, algorithms are compared to judge whether or not to establish a connection.

(Communication System)

[0078] As shown in Fig. 8, a communication system according to the fourth embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0079] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling a radio access system. Further, the switch apparatus 30 stores an identifier (e.g., an operator identifier B) which uniquely identifies an apparatus controlling the switch apparatus.

[0080] As shown in Fig. 8, the mobile station 10 includes a communication unit 11, an authentication unit 12, a judgment unit 13, a registering unit 14, a data storage unit 15, and an algorithm storage unit 18.

[0081] As shown in Fig. 9, the algorithm storage unit 18 stores, as a radio zone algorithm list, a secured algorithm used in the radio system or a non-secured algorithm used in the radio access system. As shown in Fig. 9, for example, in the radio zone, when a secret is an AES and when an integrity algorithm is an SHA-1, a security is ensured, and a new security connection (IPsec) is set to be unnecessary.

[0082] The judgment unit 13 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 13 judges whether or not to establish the connection by comparing the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system and the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus, and by comparing the algorithm used in the radio access system, and the algorithm list.

[0083] The communication unit 11, the authentication unit 12, the registering unit 14, and the data storage unit 15 are the same as those of the first embodiment, so that further description thereof is herein omitted.

(Communication Method)

[0084] Next, a communication method in accordance with the fourth embodiment is described with reference to Fig. 10.

[0085] First, the mobile station 10 stores a radio zone algorithm list (S401); the access point 20 stores the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S402); and the switch apparatus 30 stores the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus 30 (S403).

[0086] Next, the mobile station 10 performs an authentication with the access point 20 located on the radio access system, so as to exchange that a secret key and an integrity key (S404). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0087] Next, the mobile station 10 stores an algorithm for the secret and the integrity to use In the radio zone (S405). Here, the secured connection is established between the mobile station 10 and the access point 20 located on the radio access system.

[0088] Next, the mobile station 10 transmits an operator identifier request to the P-CSCF 30a (S406), and the P-CSCF 30a transmits an operator identifier response, including the operator identifier B, to the mobile station 10 (S407). Thereafter, the mobile station 10 compares the operator identifier A and the operator identifier B (S408). Subsequently, the mobile station 10 compares the algorithm used in the radio access system and the algorithm list (S409). Here, when the operator identifier

A and the operator identifier B are the same, and also when the algorithm used in the radio access system is set so as unnecessary an IPsec in the algorithm list, the mobile station 10 judges that establishing the secured connection is unnecessary. Incidentally, the processes described herein below are performed when it is judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0089] Meanwhile, processes of steps S410 to S418 are the same as those of steps S108 to S116 shown in Fig. 2, so that further description thereof is omitted.

(Operation and effects)

[0090] In accordance with the communication system, the mobile station 10, and the communication method according to the fourth embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and the identifier (e.g., the operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus, and by comparing the algorithm used in the radio access system and the algorithm list, and thereby.

[0091] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the fourth embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0092] Further, in the fourth embodiment, algorithms in the radio zone are compared, so that when a strong security connection is established, a finer control becomes possible in such a way that a new connection is not established between the mobile station 10 and the switch apparatus 30.

<Fifth Embodiment>

[0093] In the second embodiment, the mobile station 10 compares the operator identifier stored by the access point 20, the operator identifier stored by the switch apparatus 30, and the operator identifier list; however, in a fifth embodiment, a description is given for an example in which, in addition to the above comparison, algorithms are compared to judge whether or not to establish a connection.

(Communication System)

[0094] As shown in Fig. 11, a communication system according to the fifth embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0095] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling a radio access system. Further, the switch apparatus 30 stores an identifier (e.g., an operator identifier B) which uniquely identifies an apparatus controlling the switch apparatus.

[0096] As shown in Fig. 11, the mobile station 10 includes a communication unit 11, an authentication unit 12, a judgment unit 13, a registering unit 14, a data storage unit 15, an identifier list storage unit 16, and an algorithm list storage unit 18.

[0097] The judgment unit 13 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 13 judges whether or not to establish the connection by comparing an identifier list with the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus; and by comparing the algorithm used in the radio access system and an algorithm list.

[0098] The identifier list storage unit 16 is the same as that of the second embodiment so that further description thereof is herein omitted. In addition, the algorithm storage unit 18 is the same as that of the fourth embodiment so that further description thereof is herein omitted.

[0099] The communication unit 11, the authentication unit 12, the registering unit 14, and the data storage unit 15 are the same as those of the first embodiment, so that further description thereof is herein omitted.

(Communication Method)

[0100] Next, a communication method in accordance with the fifth embodiment is described with reference to Fig. 12.

[0101] First, the mobile station 10 stores a radio zone algorithm list (S501), and the operator identifier list (S502). Further, the access point 20 stores the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S503), and the switch apparatus 30 stores the identifier (e.g., an operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus 30 (S504).

[0102] Next, the mobile station 10 performs an authentication with the access point 20 located on the radio access system, so as to exchange a secret key and an integrity key (S505). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0103] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in the radio zone (S506). Here, the secured connection is established between the mobile station 10 and the access point 20 located on the radio access system.

[0104] Next, the mobile station 10 transmits an operator identifier request to the P-CSCF 30a (S507), and the P-CSCF 30a transmits an operator identifier response, including an operator identifier B, to the mobile station 10 (S508). Thereafter, the mobile station 10 compares the operator identifier list with the operator identifier A, and the operator identifier B (S509). Subsequently, the mobile station 10 compares the algorithm used in the radio access system and the algorithm list (S510). Here, when a combination of the operator identifier A and the operator identifier B is set so as unnecessary an IPsec in the operator identifier list, and also when the algorithm used in the radio access system is set so as unnecessary an IPsec in the algorithm list, the mobile station 10 judges that establishing the secured connection is unnecessary. Incidentally, the processes described herein below are performed when it is judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0105] Meanwhile, processes of steps S511 to S519 are the same as those of steps S108 to S116 shown in Fig. 2, so that further description thereof is herein omitted.

(Operation and effects)

[0106] In accordance with the communication system, the mobile station 10, and the communication method according to the fifth embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the operator identifier list with the identifer (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and the identifier (e.g., the operator identifier B) which uniquely identifies the apparatus controlling the switch apparatus, and by comparing the algorithm used in the radio access system and the algorithm list.

[0107] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the fifth embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0108] Further, in the fifth embodiment, it is possible to arbitrarily rewrite the operator identifier, and to flexibly judge whether an establishment of a connection is existed. In addition, algorithms in the radio zone are compared, so that when a strong security connection is established, a finer control becomes possible in such a way that a new connection is not established between the mobile station 10 and the switch apparatus 30.

<Sixth Embodiment>

[0109] In the third embodiment, the mobile station 10 stores the identifier which uniquely identifies the apparatus controlling the switch apparatus 30, and compares this identifier with an operator identifier that switch apparatus 30 stores; however, in a sixth embodiment, a description is given for an example in which, in addition to the above comparison, an algorithm list is compared to judge whether or not to establish a connection.

(Communication System)

[0110] As shown in Fig. 13, a communication system according to the sixth embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, It is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0111] The access point 20 stores an identifier (e.g., an operator identifier A) which uniquely identifies an apparatus controlling the radio access system.

[0112] As shown in Fig. 13, the mobile station 10 includes a communication unit 11, an authentication unit 12, a judgment unit 13, a registering unit 14, a data storage unit 15, an identifier storage unit 17, and an algorithm list storage unit 18.

[0113] The judgment unit 13 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 13 judges whether or not to establish the connection by comparing an identifier (e.g., an operator identifier C) stored by the identifier storage unit 17 and the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and by comparing the algorithm used in the radio access system and the algorithm list.

[0114] The identifier storage unit 17 is the same as that of the third embodiment so that further description thereof is herein omitted. In addition, the algorithm storage unit 18 is the same as that of the fourth embodiment so that further description thereof is herein omitted.

[0115] The communication unit 11, the authentication unit 12, the registering unit 14, and the data storage unit 15 are the same as those of the first embodiment, so that further description thereof is herein omitted.

(Communication Method)

[0116] Next, a communication method in accordance with the sixth embodiment is described with reference to Fig. 14.

[0117] First, the mobile station 10 stores a radio zone

algorithm list (S601), and the identifier (e.g., an operator identifier C) which uniquely identifies the apparatus controlling the switch apparatus 30 (S602). Further, the access point 20 stores the identifier (e.g., an operator identifier A) which uniquely identifies the apparatus controlling the radio access system (S603).

[0118] Next, the mobile station 10 performs an authentication with the access point 20 located on the radio access system, so as to exchange a secret key and an integrity key (S604). At this time, the access point 20 transmits the operator identifier A to the mobile station 10, and the mobile station 10 stores the operator identifier A.

[0119] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in a radio zone (S605). Here, the secured connection is established between the mobile station 10 and the access point 20 located on the radio access system.

[0120] Next, the mobile station 10 compares the operator identifier C and the operator identifier A (S606). Subsequently, the mobile station 10 compares the algorithm used in the radio access system and the algorithm list (S607). Here, when the operator identifier C and the operator identifier A are the same, and also when the algorithm used in the radio access system is set so as unnecessary an IPsec In the algorithm list, the mobile station 10 judges that establishing the secured connection is unnecessary. Incidentally, the processes described herein below are performed when it is judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0121] Meanwhile, processes of steps S608 to S616 are the same as those of steps S108 to S116 shown in Fig. 2, so that further description thereof is omitted.

(Operation and effects)

[0122] In accordance with the communication system, the mobile station 10, and the communication method according to the sixth embodiment, the mobile station 10 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 by comparing the identifier (e.g., the operator identifier C) which uniquely identifies the apparatus controlling the switch apparatus and the identifier (e.g., the operator identifier A) which uniquely identifies the apparatus controlling the radio access system, and by comparing the algorithm used in the radio access system and the algorithm list.

[0123] Therefore, in accordance with the communication system, the mobile station 10, and the communication method according to the sixth embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0124] Further, in the sixth embodiment, it is unnecessary to receive an operator identifier from the switch apparatus 30, so it is possible to shorten the time of a connection delay and reduce the process load on a mobile station and a switch apparatus, even more. In addition, in the sixth embodiment, algorithms in the radio zone are compared, so that when a strong security connection is established, a finer control becomes possible in such a way that a new connection is not established between the mobile station 10 and the switch apparatus 30.

<Seventh Embodiment>

[0125] In a seventh embodiment, a description is given for an example in which a switch apparatus stores a range of IP addresses that its own radio access system assigns, and compares it with the IP address of a mobile station, and thereby judges whether or not to establish a connection.

(Communication System)

[0126] As shown in Fig. 15, a communication system according to the seventh embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, it is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0127] As shown in Fig. 15, the switch apparatus 30 includes a communication unit 31, an authentication unit 32, a judgment unit 33, a registering unit 34, a data storage unit 35, and an address list storage unit 36.

[0128] The communication unit 31 performs communication with the mobile station 10 so as to perform transmisslon/reception of an IP address, a user ID, an authentication request, and signals of various kinds.

[0129] The authentication unit 32 performs an authentication between the mobile station 10 and the switch apparatus 30.

[0130] The judgment unit 33 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 33 judges whether or not to establish the connection by comparing the address of the mobile station 10 transmitted from the mobile station 10 and an address list stored by the address list storage unit 36.

[0131] The registering unit 34 performs an SIP registration on the mobile station 10.

[0132] The data storage unit 35 stores IP addresses, data in the middle of a transmission, and the like, which have been received.

[0133] As shown in Fig. 16, the address list storage unit 36 stores the address list indicating the range of IP addresses that the radio access system on which the

switch apparatus 30 is located to assigns.

(Communication Method)

[0134] Next, a communication method in accordance with the seventh embodiment is described with reference to Fig. 17. It is assumed that the switch apparatus 30 stores an IP address list.

[0135] First, the mobile station 10 performs the authentication with the access point 20 located on the radio access system, so as to exchange a secret key and an integrity key (S701).

[0136] Next, the mobile station 10 stores an algorithm for the secret and the integrity to be used in a radio zone (S702). Here, the secured connection is established between the mobile station 10, and the access point 20 located on the radio access system.

[0137] Thereafter, the mobile station 10 transmits the user ID, the authentication request, the IPsec security association, and the like to the P-CSCF 30a so as to perform the SIP registration (S703). Next, the P-CSCF 30a transmits an IPsec necessary/unnecessary acknowledgement request, including the IP address, to the mobile station 10 (S704).

[0138] Next, the judgment unit 33 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30 (S705). To be more precise, the judgment unit 33 judges whether or not to establish the connection by comparing the address of the mobile station 10 transmitted from the mobile station 10 and the IP address list stored by the address list storage unit 36. For example, the judgment unit 33 judges that the IP address of the mobile station transmitted from the mobile station 10 is an IP address that its own radio access system has assigned, when the IP address is in an IP address range shown in Fig. 16, and judges that establishing the secured connection is unnecessary.

[0139] Thereafter, the judgment unit 33 transmits a response, notifying that IPsec is unnecessary, to the P-CSCF 30a (S706). Incidentally, the processes described herein below are performed when it is judged that the connection is unnecessary, when the connection is necessary, the connection is established by performing the same procedure as a conventional procedure.

[0140] Meanwhile, processes of steps S707 to S714 are the same as those of steps S109 to S116 shown in Fig. 2, so that further description thereof is omitted.

(Operation and effects)

[0141] In accordance with the communication system, the switch apparatus 30, and the communication method according to the seventh embodiment, the switch apparatus 30 compares the address of the mobile station 10 and the IP address list stored by the address list storage unit 36, and thereby judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. When the address of the mobile station 10 is included In the address list, the secured connection is already established between the mobile station 10 and the switch apparatus 30, so that it is judged that establishing a new connection is unnecessary.

[0142] Therefore, in accordance with the communication system, the switch apparatus 30, and the communication method according to the seventh embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

<Eighth Embodiment>

[0143] In the seventh embodiment, the switch apparatus 30 compares the address of the mobile station 10 and the address list; however, in an eighth embodiment, a description is given for an example in which, in addition to the above comparison, algorithm lists are compared to judge whether or not to establish a connection.

(Communication System)

[0144] As shown in Fig. 18, a communication system according to the eighth embodiment includes a mobile station 10, an access point 20 (e.g., a base station) located on a radio access system, and a switch apparatus 30 (e.g., an IMS apparatus) connected to the radio access system. In this communication system, It is assumed that a secured (a secret/an integrity) connection is established between the mobile station 10 and the access point 20.

[0145] As shown in Fig. 18, the switch apparatus 30 includes a communication unit 31, an authentication unit 32, a judgment unit 33, a registering unit 34, a data storage unit 35, an address list storage unit 36, and an algorithm list storage unit 37.

[0146] The judgment unit 33 judges whether or not to establish the secured connection between the mobile station 10 and the switch apparatus 30. To be more precise, the judgment unit 33 judges whether or not to establish the connection by comparing the address of the mobile station 10 transmitted from the mobile station 10, and an address list, and by comparing the algorithm used in the radio access system and the algorithm list.

[0147] The communication unit 31, the authentication unit 32, the registering unit 34, the data storage unit 35, and the address list storage unit 36 are the same as those of the seventh embodiment, so that description thereof is herein omitted. In addition, the algorithm storage unit 37 is the same as that of the fourth embodiment so that further description thereof is herein omitted.

(Communication Method)

[0148] Next, a communication method in accordance

with the eighth embodiment is described with reference to Fig. 19. It is assumed that the switch apparatus 30 stores an IP address list and a radio zone algorithm list.

[0149] Meanwhile, processes of steps S801 to S804 are the same as those of steps S701 to S704 shown in Fig. 17, so that further description thereof is omitted.

[0150] The Judgment unit 33 judges whether or not to establish a secured connection between the mobile station 10 and the switch apparatus 30 (S805 and S806). To be more precise, the judgment unit 33 compares the address of the mobile station 10 transmitted from the mobile station 10 and the IP address list stored by the address list storage unit 36 (S805). Next, the judgment unit 33 compares the algorithm used in the radio access system, and the radio zone algorithm list (S806). Here, when the IP address of the mobile station 10 corresponds to the IP address list and also when an algorithm used in the radio access system is set so as not to need an IPsec in the radio zone algorithm list, the switch apparatus 30 judges that it is unnecessary to establish a secured connection. Incidentally, the following processes are those in the case where it is judged that establishing the connection is unnecessary, but when a connection is necessary, it is established in the same procedure as a conventional procedure.

[0151] Meanwhile, processes of steps S807 to S815 are the same as those of steps S706 to S714 shown in Fig. 17, so that further description thereof is omitted.

[0152] In accordance with the communication system, the switch apparatus 30, and the communication method according to the eighth embodiment, the switch apparatus 30judges whether or not to establish a secured connection between the mobile station 10 and the switch apparatus 30 by comparing the address of the mobile station 10 and the IP address list, and by comparing the algorithm used in the radio access system, and the radio zone algorithm list.

[0153] Therefore, in accordance with the communication system, the switch apparatus 30, and the communication method according to the eighth embodiment, it is possible to skip an encryption process of the IMS and to eliminate an unnecessary encryption process. Therefore, it is possible to shorten the time of a connection delay and to reduce a process load on the mobile station and the network.

[0154] In addition, in the eighth embodiment, algorithms in the radio zone are compared, so that when a strong security connection is established, a finer control becomes possible in such a way that a new connection is not established between the mobile station 10 and the switch apparatus 30.

<Other Embodiment>

[0155] The present invention has been set forth in the above described embodiments. But it should not be understood that the discussion and the drawings constituting a part of this disclosure are interpreted to limit the present invention. It is apparent to those skilled in the art that various alternatives, modifications, and the practices can be achieved based on this disclosure.

[0156] For example, in the description of the first to sixth embodiments, the identifier which uniquely identifies the apparatus controlling the radio access system, and the identifier which uniquely identifies the apparatus controlling the switch apparatus have been compared, but the identifier which uniquely identifies the radio access system, and the identifier which uniquely identifies the switch apparatus may be compared.

[0157] Further, in the description of the seventh and eight embodiments, the judgment unit 33, the address list storage unit 36, the algorithm list storage unit 37, and the like are located on one switch apparatus 30, but each of these units may be located on an apparatus other than the switch apparatus.

[0158] As described above, the present invention naturally includes various embodiments and the like which are not herein described. Accordingly, the scope of the present invention is indicated only by the appended claims being relevant to the foregoing description.

[Industrial Applicability]

[0159] In accordance with the present invention, it is possible to provide a communication system, a mobile station, a switch apparatus, and a communication method, which can shorten a time of delay in connecting the mobile station and a network, and can reduce a process load on the mobile station and the network.

Claims

1. A communication system for establishing a secured first connection between a mobile station and an access point located on a radio access system, comprising:

   a judgment unit configured to judge whether or not to establish a secured second connection between the mobile station and a switch apparatus connected to the radio access system.

2. The communication system according to claim 1, wherein
   the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which is received from the switch apparatus and which uniquely identifies an apparatus controlling the switch apparatus.

3. The communication system according to claim 1, further comprising:

an identifier list storage unit configured to store an identifier list which is a combination of an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which uniquely identifies an apparatus controlling the switch apparatus; wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing the identifier list, with the identifier which is received from the access point and which uniquely identifies the apparatus controlling the radio access system, and the identifier which is received from the switch apparatus and which uniquely identifies the apparatus controlling the switch apparatus.

4. The communication system according to claim 1, wherein the mobile station further comprising an identifier storage unit configured to store an identifier which uniquely identifies an apparatus controlling the switch apparatus, and
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing an identifier which is stored in the identifier storage unit, and an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system.

5. The communication system according to claim 1, further comprising an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system or a non-secured algorithm used in the radio access system, wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and an identifier which is received from the switch apparatus and which uniquely identifies an apparatus controlling the switch apparatus, and by comparing the algorithm list and the algorithm used in the radio access system.

6. The communication system according to claim 1, further comprising:

an identifier list storage unit configured to store an identifier list which is a combination of an identifier which is received from the access point and which uniquely identifies an apparatus controlling the switch apparatus, and an identifier which uniquely identifies an apparatus controlling the switch apparatus; and
algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used In the radio access system or a non-secured algorithm used In the radio access system, wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing the identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, the identifier which is received from the switch apparatus and which uniquely identifies an apparatus controlling the switch apparatus, and the identifier list, and by comparing the algorithm list and the algorithm used in the radio access system.

7. The communication system according to claim 1, wherein the mobile station further comprising:

an identifier storage unit configured to store an identifier which uniquely identifies an apparatus controlling the switch apparatus; and
an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system or a non-secured algorithm used in the radio access system; wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing an identifier which is stored in the identifier storage unit, and an identifier which is received from the access point and which uniquely identifies an apparatus controlling the radio access system, and by comparing the algorithm list and the algorithm used in the radio access system.

8. The communication system according to claim 1, further comprising:

an address list storage unit configured to store an address list which indicates a range of an address assigned by the radio access system on which the switch apparatus is located; wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing the address list and an address of the mobile station which is transmitted from the mobile station.

9. The communication system according to claim 1, further comprising:

an address list storage unit configured to store an address list which indicates a range of an address assigned by the radio access system on which the switch apparatus is located; and
an algorithm list storage unit configured to store, as an algorithm list, a secured algorithm used in the radio access system or a non-secured algo-

rithm used in the radio access system on which the access point is located; wherein
the judgment unit is configured to judge whether or not to establish the secured second connection, by comparing the address list and an address of the mobile station which is transmitted from the mobile station, and by comparing the algorithm list and the algorithm used in the radio access system on which the access point is located.

10. A mobile station for establishing a secured first connection with an access point located on a radio access system, comprising:

a judgment unit configured to judge whether or not to establish a secured second connection between the mobile station and a switch apparatus connected to the radio access system.

11. A switch apparatus connected to a radio access system in a communication system for establishing a secured first connection between a mobile station and an access point located on the radio access system, comprising:

a judgment unit configured to judge whether or not to establish a secured second connection between the mobile station and the switch apparatus.

12. A communication method in a communication system provided with a mobile station, an access point located on a radio access system, and a switch apparatus connected to the radio access system, comprising:

establishing a first secured connection between the mobile station and the access point; and
determining whether or not to establish a secured second connection between the mobile station and the switch apparatus.

FIG. 1

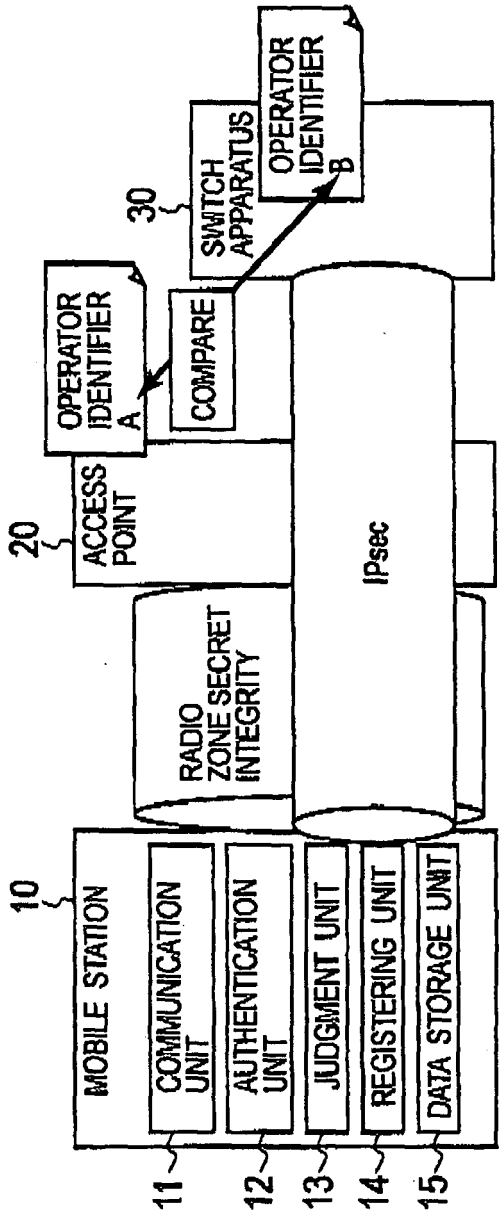

10
MOBILE STATION
COMMUNICATION UNIT
AUTHENTICATION UNIT
JUDGMENT UNIT
REGISTERING UNIT
DATA STORAGE UNIT
11
12
13
14
15
RADIO ZONE SECRET INTEGRITY
20
ACCESS POINT
OPERATOR IDENTIFIER A
COMPARE
IPsec
30
SWITCH APPARATUS
OPERATOR IDENTIFIER B

FIG. 2

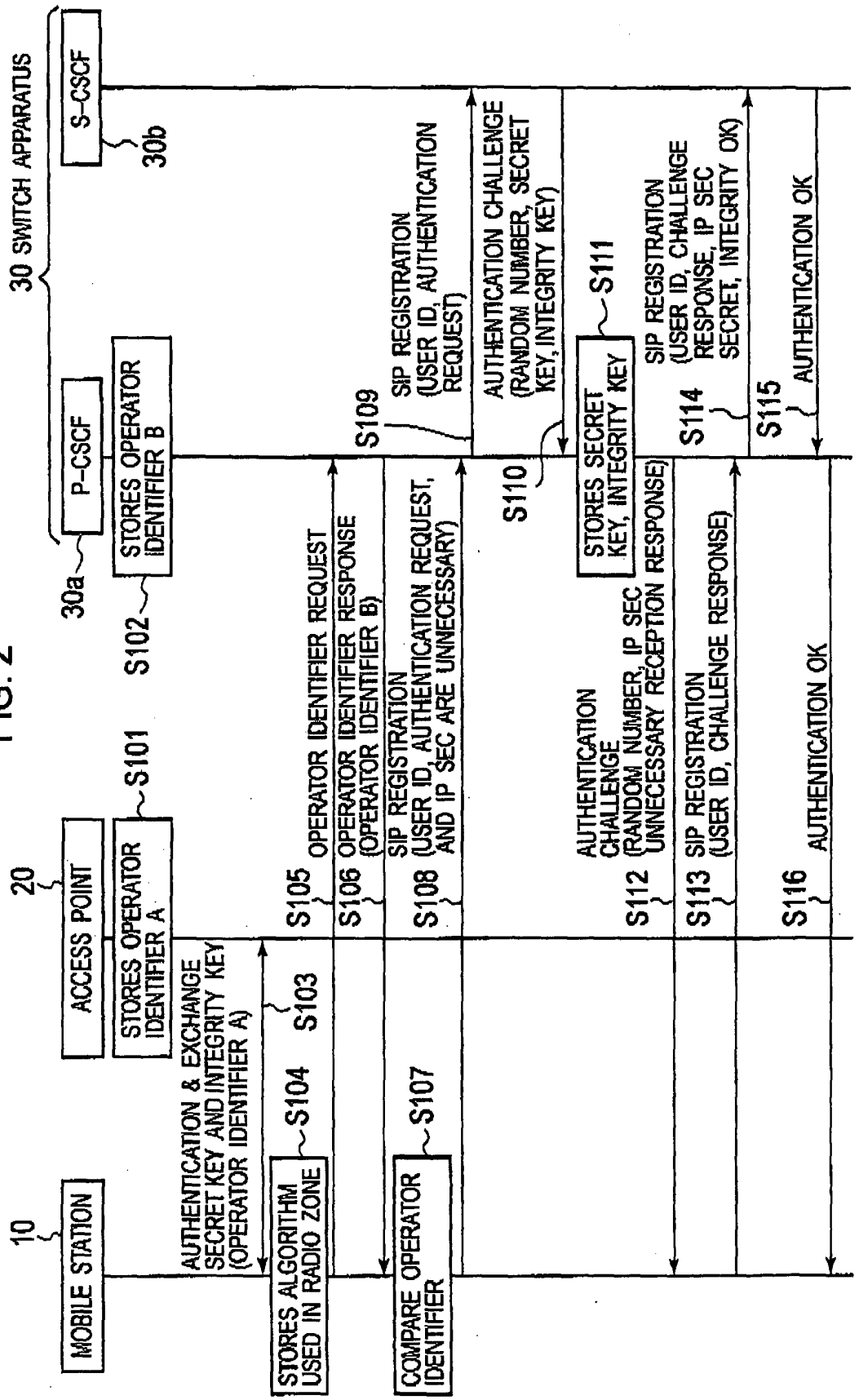

10
MOBILE STATION
20
ACCESS POINT
30 SWITCH APPARATUS
30a
P-CSCF
30b
S-CSCF
STORES OPERATOR IDENTIFIER A
S101
STORES OPERATOR IDENTIFIER B
S102
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S103
STORES ALGORITHM USED IN RADIO ZONE
S104
S105 OPERATOR IDENTIFIER REQUEST
S106 OPERATOR IDENTIFIER RESPONSE (OPERATOR IDENTIFIER B)
COMPARE OPERATOR IDENTIFIER
S107
S108 SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S109 SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S110
STORES SECRET KEY, INTEGRITY KEY
S111
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
S112
S113 SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S114 SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S115
AUTHENTICATION OK
S116
AUTHENTICATION OK

FIG. 3

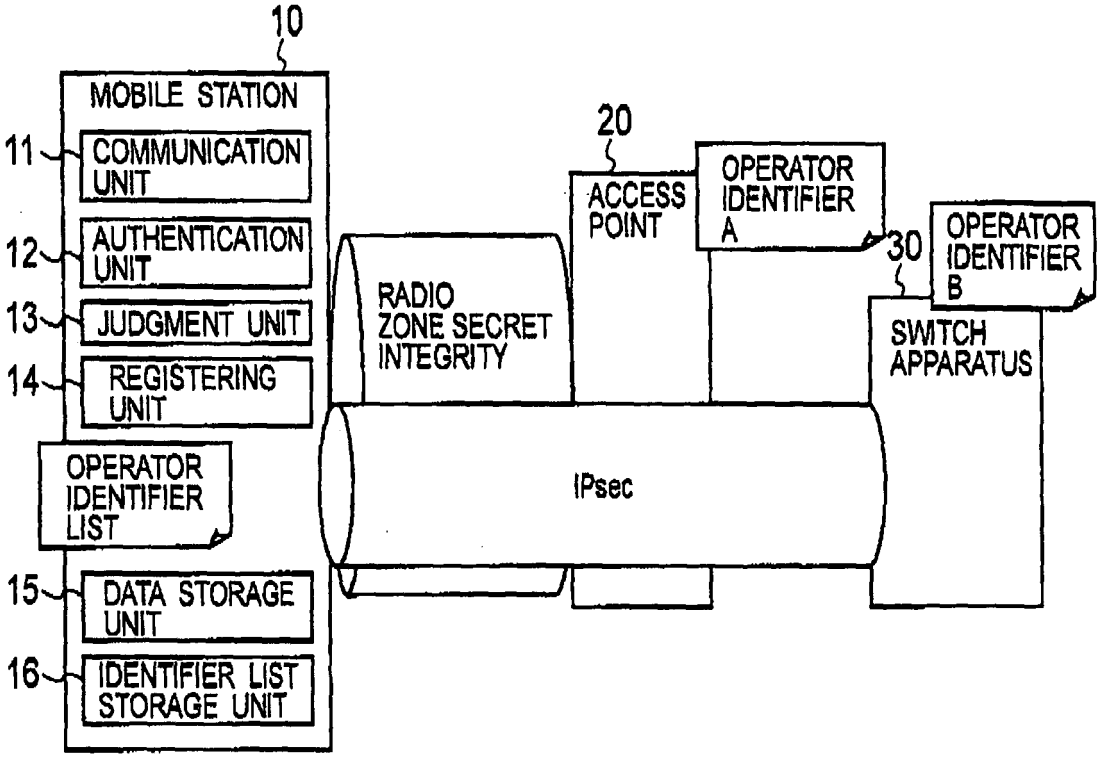


FIG. 4

ACCESS POINT	SWITCH APPARATUS	IP sec
OPERATOR X	OPERATOR X	NECESSARY
OPERATOR X	OPERATOR Z	UNNECESSARY
OPERATOR Y	OPERATOR X	NECESSARY

FIG. 5

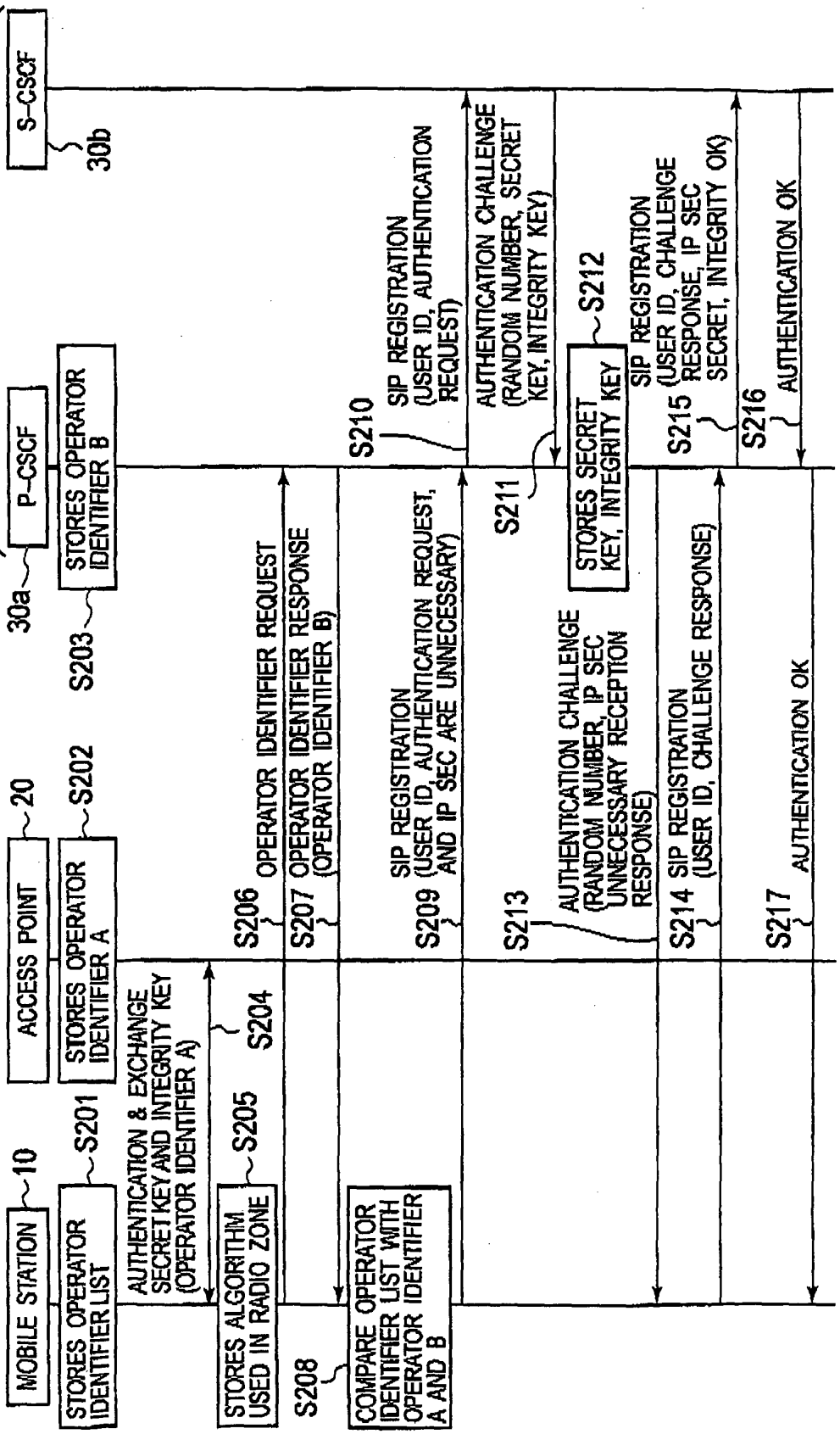

30 SWITCH APPARATUS
MOBILE STATION
10
ACCESS POINT
20
30a
P-CSCF
S-CSCF
30b
STORES OPERATOR IDENTIFIER LIST
S201
STORES OPERATOR IDENTIFIER A
S202
STORES OPERATOR IDENTIFIER B
S203
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S204
STORES ALGORITHM USED IN RADIO ZONE
S205
S206 OPERATOR IDENTIFIER REQUEST
S207 OPERATOR IDENTIFIER RESPONSE (OPERATOR IDENTIFIER B)
S208
COMPARE OPERATOR IDENTIFIER LIST WITH OPERATOR IDENTIFIER A AND B
S209 SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S210 SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S211
STORES SECRET KEY, INTEGRITY KEY
S212
S213 AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S214 SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S215
S216 AUTHENTICATION OK
S217 AUTHENTICATION OK

FIG. 6

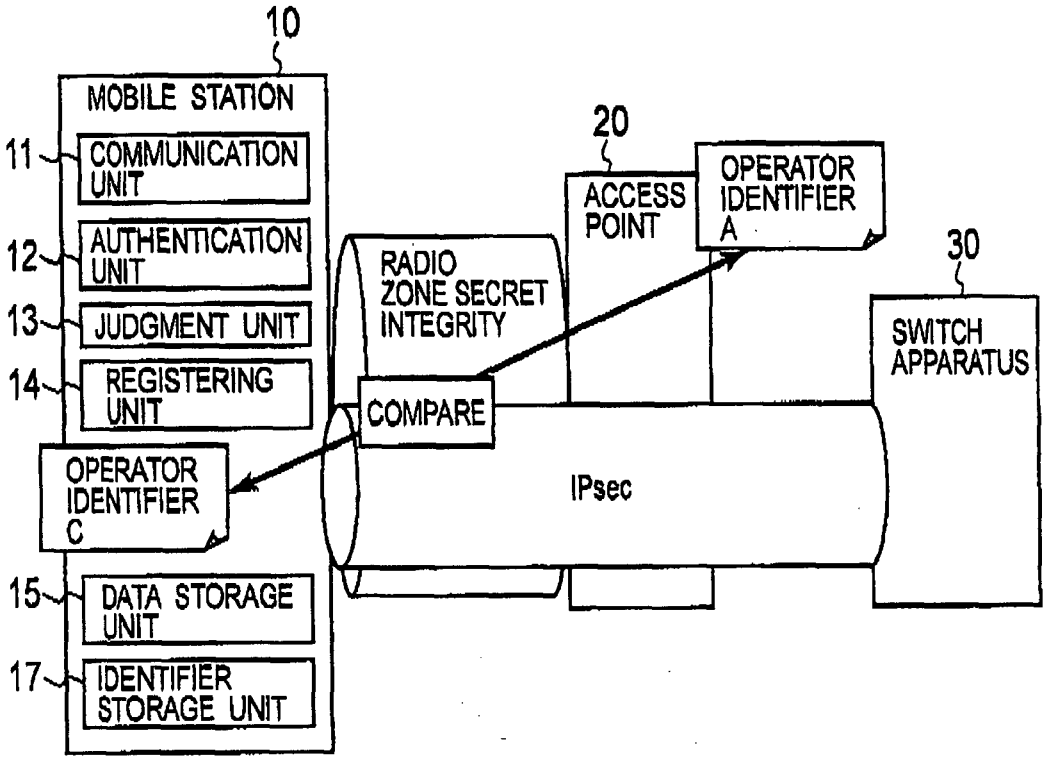

10
MOBILE STATION
11
COMMUNICATION UNIT
12
AUTHENTICATION UNIT
13
JUDGMENT UNIT
14
REGISTERING UNIT
OPERATOR IDENTIFIER C
15
DATA STORAGE UNIT
17
IDENTIFIER STORAGE UNIT
RADIO ZONE SECRET INTEGRITY
COMPARE
20
ACCESS POINT
OPERATOR IDENTIFIER A
30
SWITCH APPARATUS
IPsec

FIG. 7

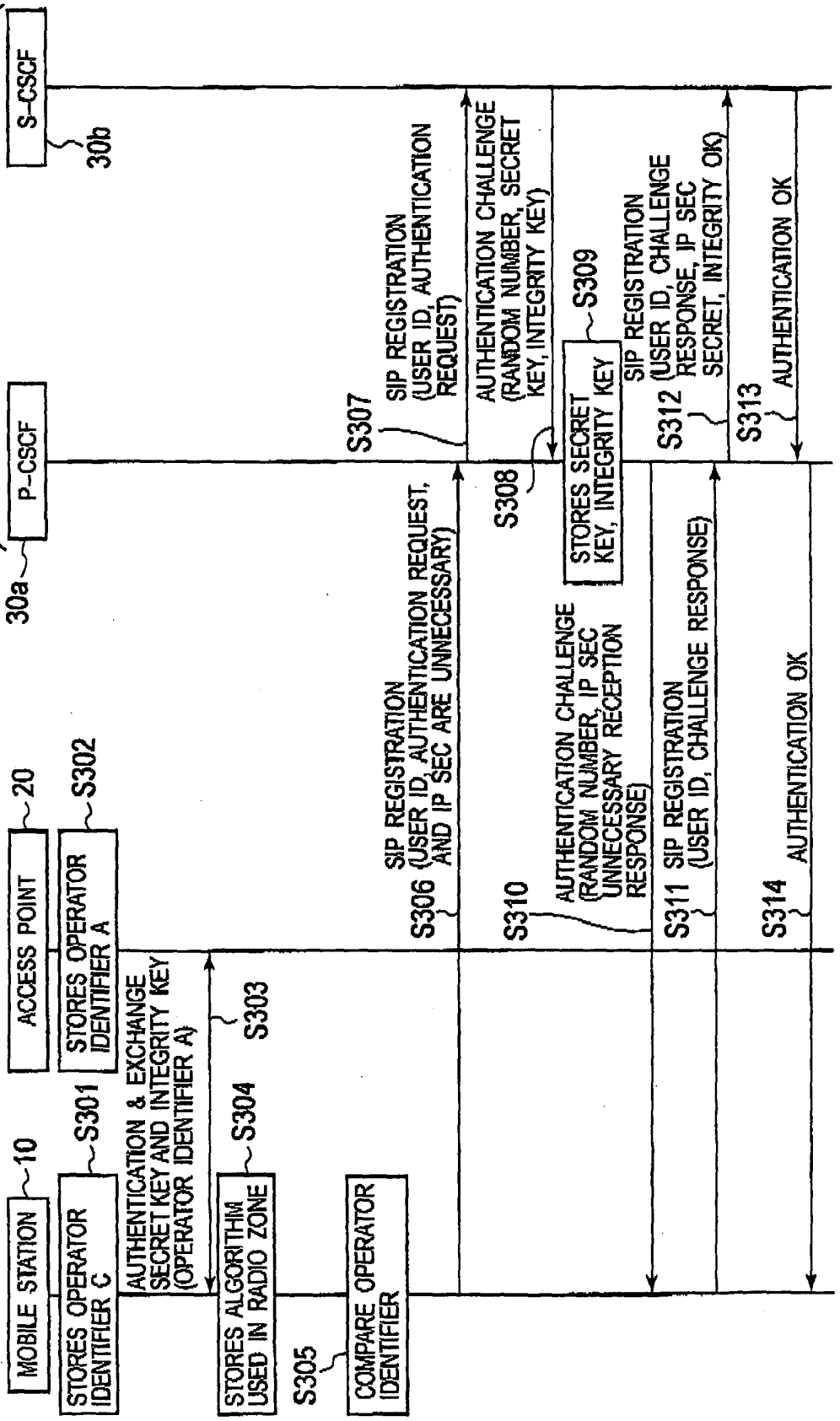

30 SWITCH APPARATUS
30a
30b
MOBILE STATION
10
ACCESS POINT
20
P-CSCF
S-CSCF
STORES OPERATOR IDENTIFIER C
S301
STORES OPERATOR IDENTIFIER A
S302
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S303
STORES ALGORITHM USED IN RADIO ZONE
S304
COMPARE OPERATOR IDENTIFIER
S305
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S306
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S307
STORES SECRET KEY, INTEGRITY KEY
S308
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S309
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
S310
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S311
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S312
AUTHENTICATION OK
S313
AUTHENTICATION OK
S314

FIG. 8

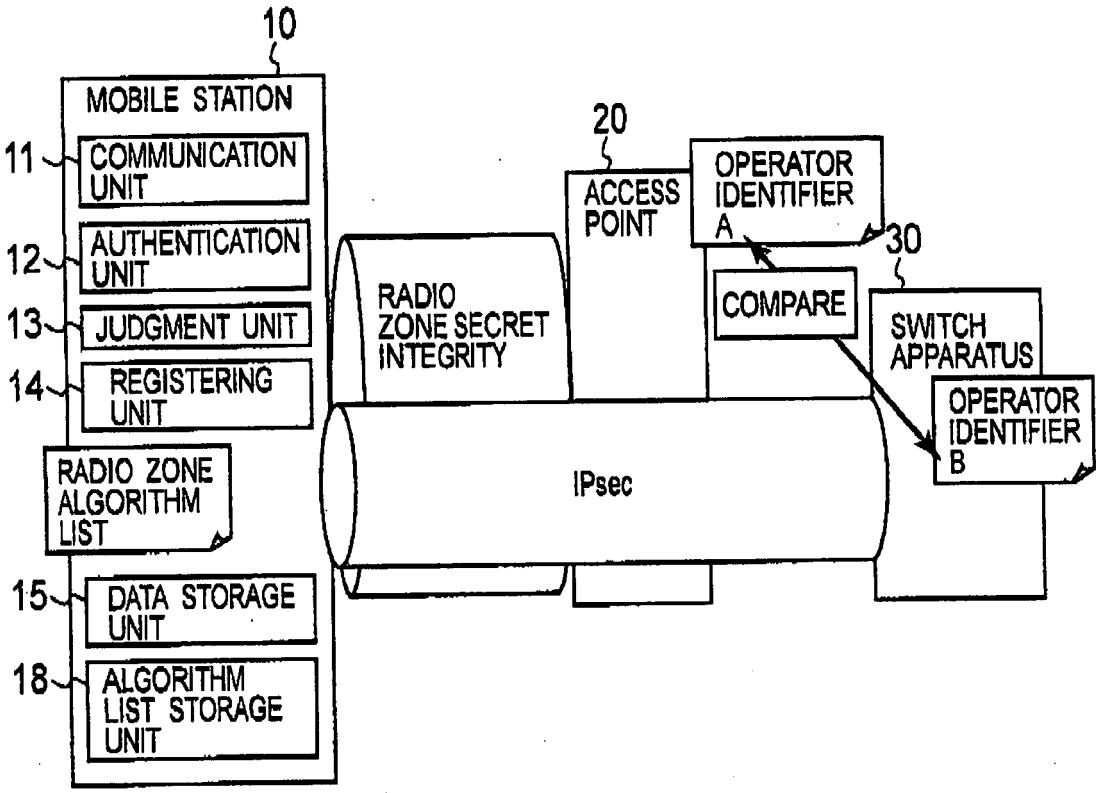


FIG. 9

SECRET	INTEGRITY	IP sec
AES	SHA-1	UNNECESSARY
3DES	SHA-1	UNNECESSARY
DES	MD5	NECESSARY

FIG. 10

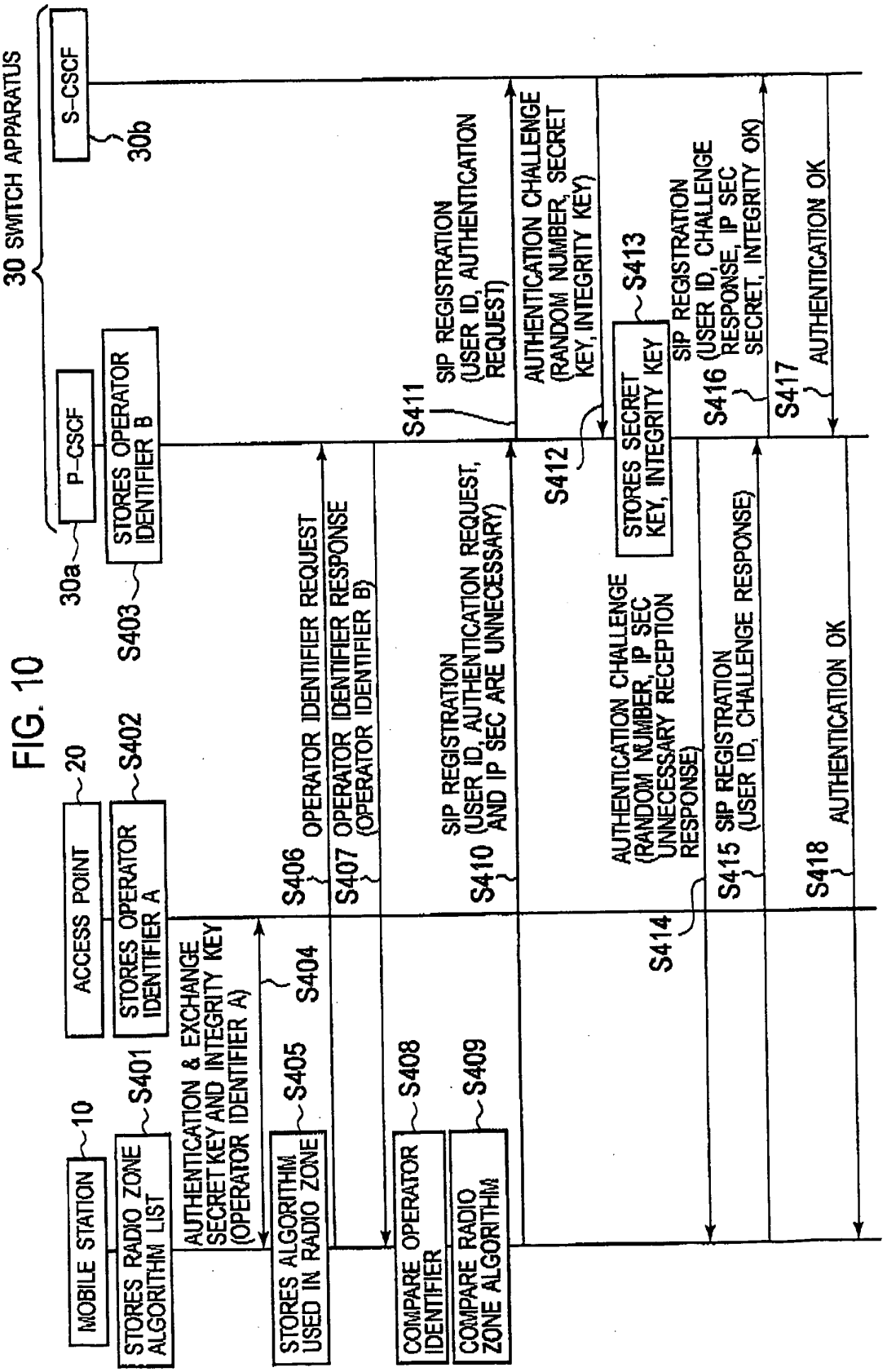

30 SWITCH APPARATUS
MOBILE STATION
10
ACCESS POINT
20
P-CSCF
30a
S-CSCF
30b
STORES RADIO ZONE ALGORITHM LIST
S401
STORES OPERATOR IDENTIFIER A
S402
STORES OPERATOR IDENTIFIER B
S403
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S404
STORES ALGORITHM USED IN RADIO ZONE
S405
OPERATOR IDENTIFIER REQUEST
S406
OPERATOR IDENTIFIER RESPONSE (OPERATOR IDENTIFIER B)
S407
COMPARE OPERATOR IDENTIFIER
S408
COMPARE RADIO ZONE ALGORITHM
S409
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S410
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S411
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S412
STORES SECRET KEY, INTEGRITY KEY
S413
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
S414
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S415
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S416
AUTHENTICATION OK
S417
AUTHENTICATION OK
S418

FIG. 11

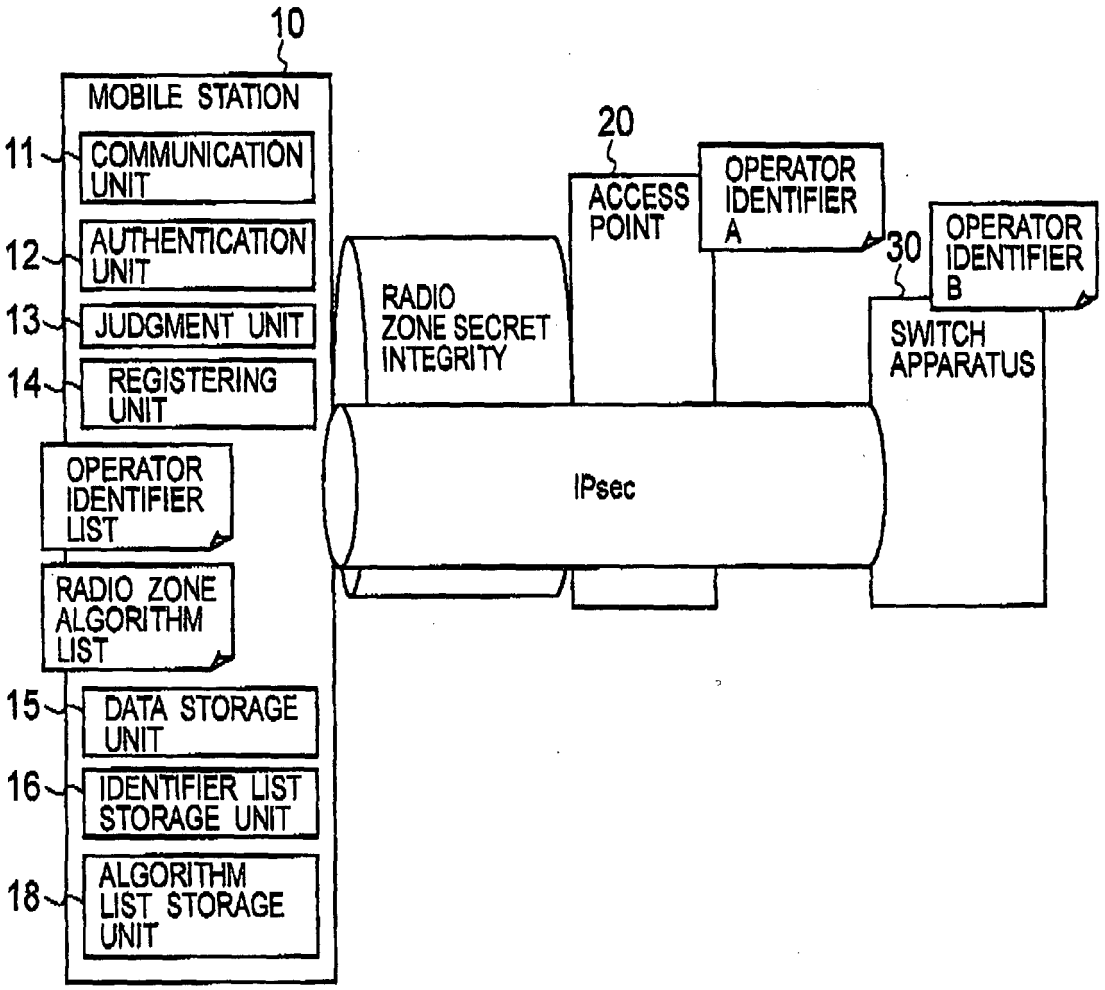

10
MOBILE STATION
11
COMMUNICATION UNIT
12
AUTHENTICATION UNIT
13
JUDGMENT UNIT
14
REGISTERING UNIT
OPERATOR IDENTIFIER LIST
RADIO ZONE ALGORITHM LIST
15
DATA STORAGE UNIT
16
IDENTIFIER LIST STORAGE UNIT
18
ALGORITHM LIST STORAGE UNIT
RADIO ZONE SECRET INTEGRITY
20
ACCESS POINT
OPERATOR IDENTIFIER A
30
OPERATOR IDENTIFIER B
SWITCH APPARATUS
IPsec

FIG. 12

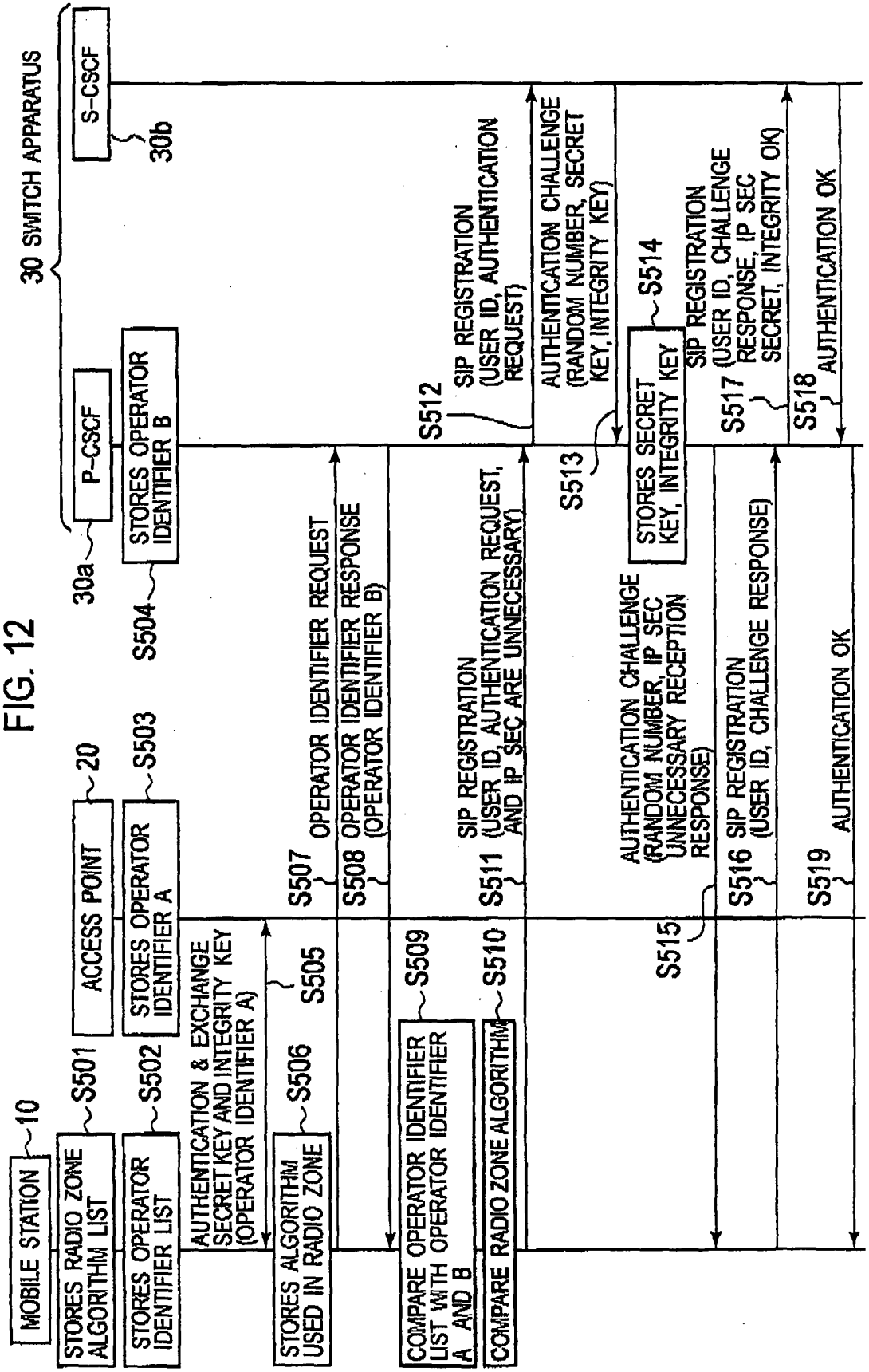

MOBILE STATION
10
30 SWITCH APPARATUS
ACCESS POINT
20
P-CSCF
30a
S-CSCF
30b
STORES RADIO ZONE ALGORITHM LIST
S501
STORES OPERATOR IDENTIFIER LIST
S502
STORES OPERATOR IDENTIFIER A
S503
STORES OPERATOR IDENTIFIER B
S504
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S505
STORES ALGORITHM USED IN RADIO ZONE
S506
OPERATOR IDENTIFIER REQUEST
S507
OPERATOR IDENTIFIER RESPONSE (OPERATOR IDENTIFIER B)
S508
COMPARE OPERATOR IDENTIFIER LIST WITH OPERATOR IDENTIFIER A AND B
S509
COMPARE RADIO ZONE ALGORITHM
S510
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S511
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S512
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S513
STORES SECRET KEY, INTEGRITY KEY
S514
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
S515
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S516
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S517
AUTHENTICATION OK
S518
AUTHENTICATION OK
S519

FIG. 13

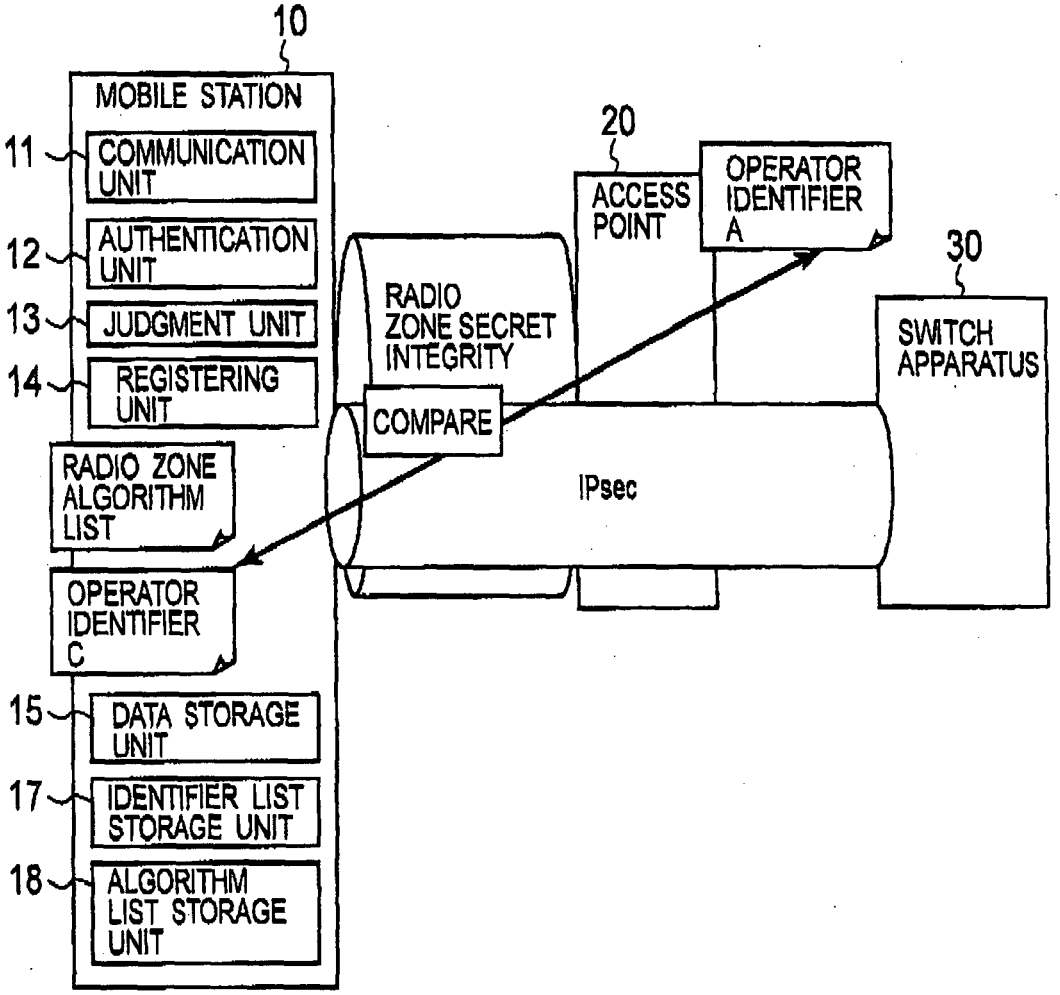

10
MOBILE STATION
11
COMMUNICATION UNIT
12
AUTHENTICATION UNIT
13
JUDGMENT UNIT
14
REGISTERING UNIT
RADIO ZONE ALGORITHM LIST
OPERATOR IDENTIFIER C
15
DATA STORAGE UNIT
17
IDENTIFIER LIST STORAGE UNIT
18
ALGORITHM LIST STORAGE UNIT
20
ACCESS POINT
OPERATOR IDENTIFIER A
30
SWITCH APPARATUS
RADIO ZONE SECRET INTEGRITY
COMPARE
IPsec

FIG. 14

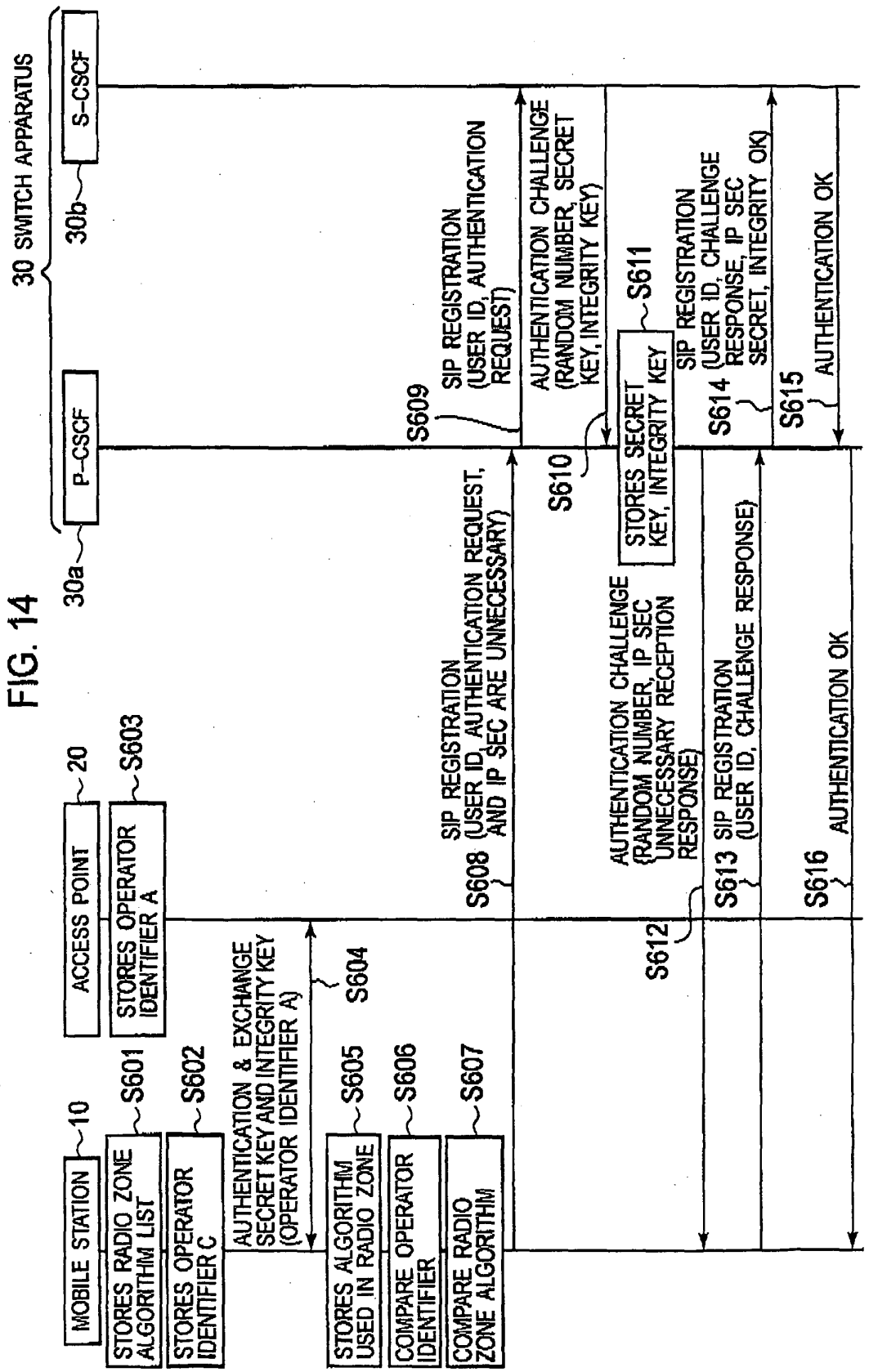

30 SWITCH APPARATUS
30a
30b
P-CSCF
S-CSCF
MOBILE STATION
10
ACCESS POINT
20
STORES RADIO ZONE ALGORITHM LIST
S601
STORES OPERATOR IDENTIFIER C
S602
STORES OPERATOR IDENTIFIER A
S603
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S604
STORES ALGORITHM USED IN RADIO ZONE
S605
COMPARE OPERATOR IDENTIFIER
S606
COMPARE RADIO ZONE ALGORITHM
S607
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, AND IP SEC ARE UNNECESSARY)
S608
S609
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S610
STORES SECRET KEY, INTEGRITY KEY
S611
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC UNNECESSARY RECEPTION RESPONSE)
S612
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE)
S613
S614
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
AUTHENTICATION OK
S615
AUTHENTICATION OK
S616

FIG. 15

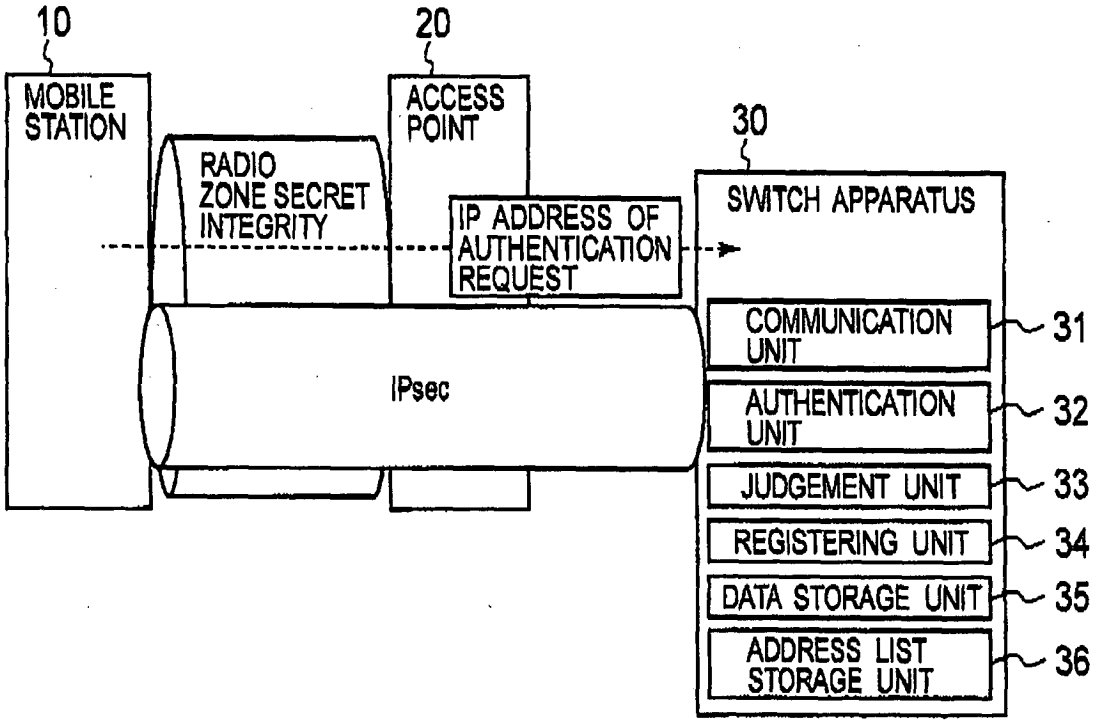


FIG. 16

	RANGE OF IP ADDRESSES
RADIO ACCESS SYSTEM A	10.0.0.0~10.1.1.1
RADIO ACCESS SYSTEM B	10.1.1.1~10.2.2.2

FIG. 17

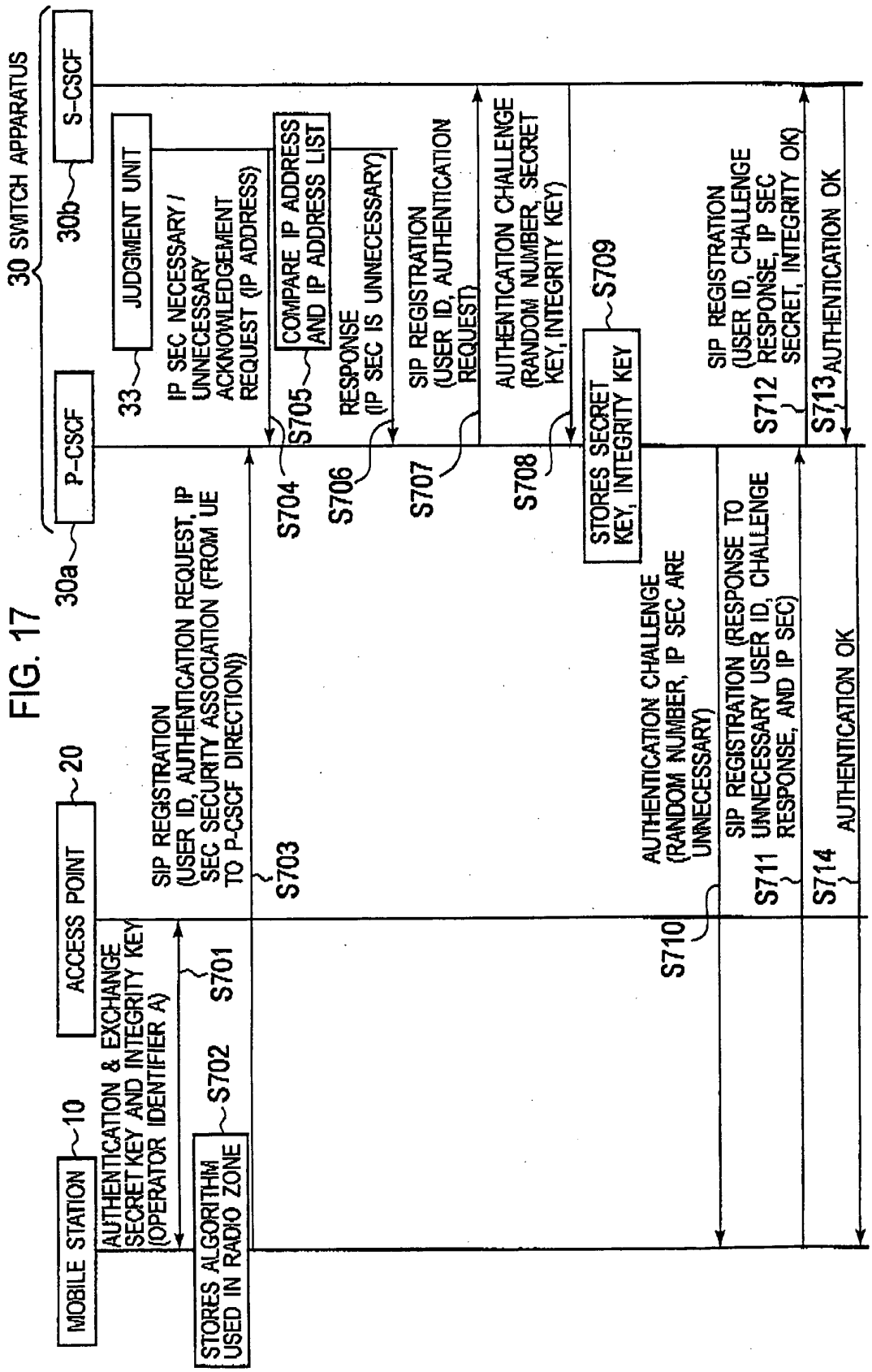

30 SWITCH APPARATUS
30a
30b
MOBILE STATION
10
ACCESS POINT
20
P-CSCF
33
JUDGMENT UNIT
S-CSCF
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S701
STORES ALGORITHM USED IN RADIO ZONE
S702
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, IP SEC SECURITY ASSOCIATION (FROM UE TO P-CSCF DIRECTION))
S703
IP SEC NECESSARY / UNNECESSARY ACKNOWLEDGEMENT REQUEST (IP ADDRESS)
S704
COMPARE IP ADDRESS AND IP ADDRESS LIST
S705
RESPONSE (IP SEC IS UNNECESSARY)
S706
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S707
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S708
STORES SECRET KEY, INTEGRITY KEY
S709
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC ARE UNNECESSARY)
S710
SIP REGISTRATION (RESPONSE TO UNNECESSARY USER ID, CHALLENGE RESPONSE, AND IP SEC)
S711
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S712
AUTHENTICATION OK
S713
AUTHENTICATION OK
S714

FIG. 18

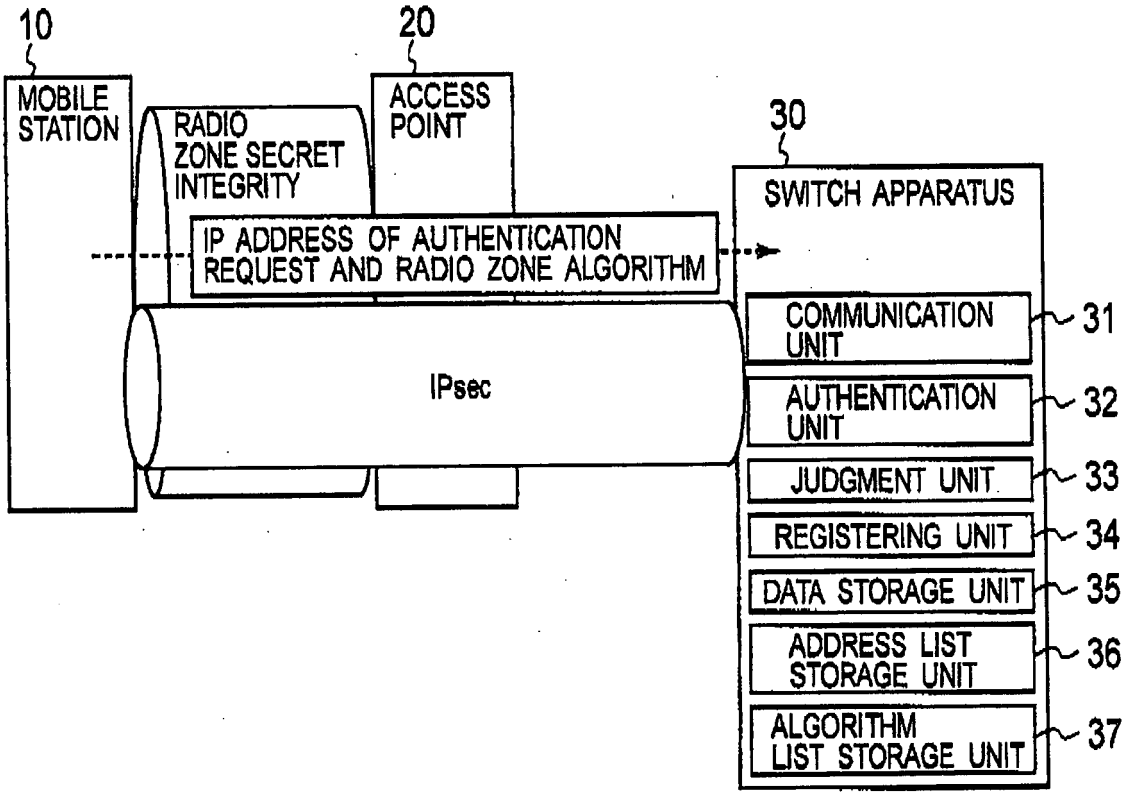

10
MOBILE STATION
20
ACCESS POINT
RADIO ZONE SECRET INTEGRITY
30
SWITCH APPARATUS
IP ADDRESS OF AUTHENTICATION REQUEST AND RADIO ZONE ALGORITHM
IPsec
COMMUNICATION UNIT
31
AUTHENTICATION UNIT
32
JUDGMENT UNIT
33
REGISTERING UNIT
34
DATA STORAGE UNIT
35
ADDRESS LIST STORAGE UNIT
36
ALGORITHM LIST STORAGE UNIT
37

FIG. 19

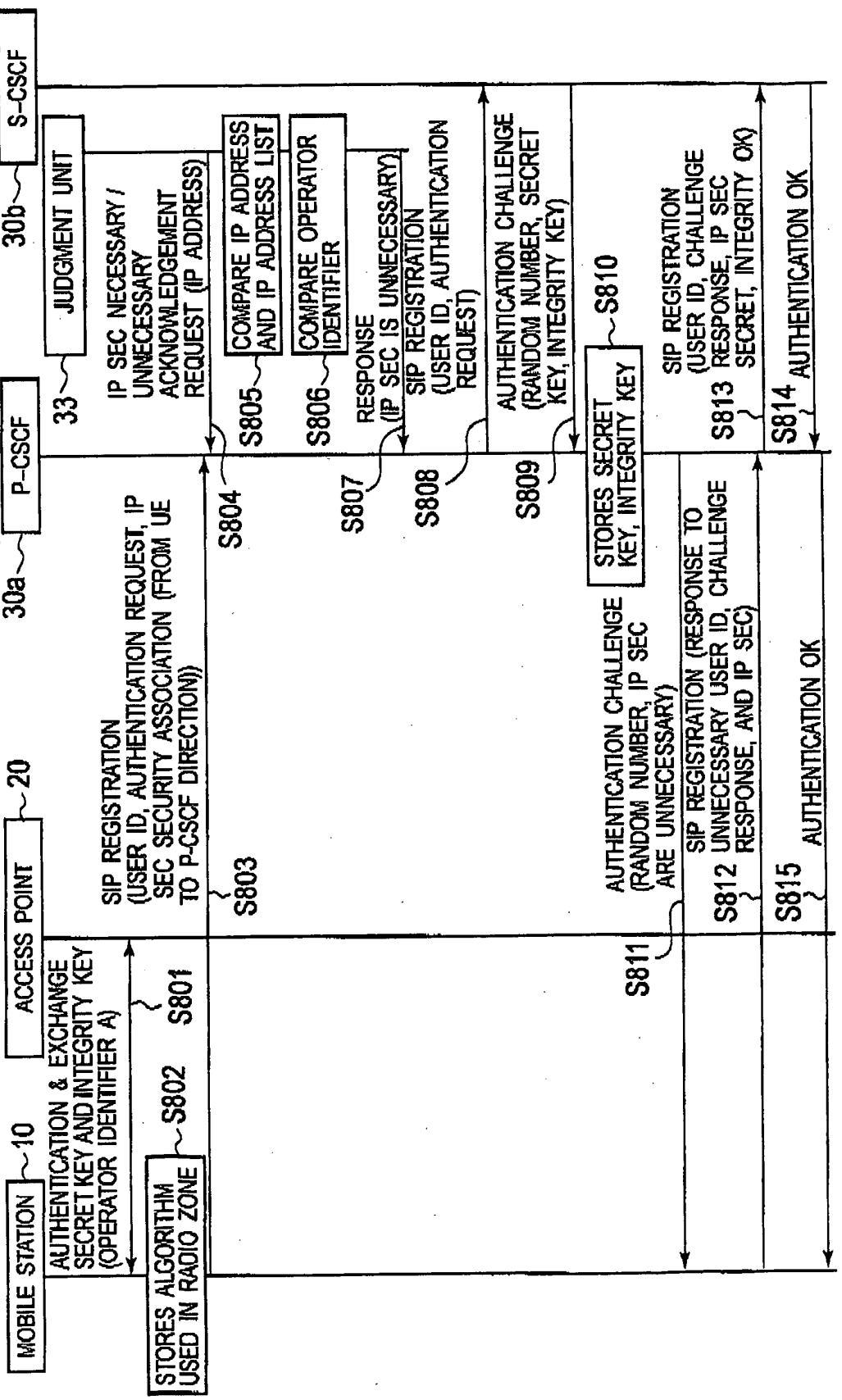

30 SWITCH APPARATUS
MOBILE STATION
10
ACCESS POINT
20
P-CSCF
30a
JUDGMENT UNIT
33
S-CSCF
30b
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY (OPERATOR IDENTIFIER A)
S801
STORES ALGORITHM USED IN RADIO ZONE
S802
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, IP SEC SECURITY ASSOCIATION (FROM UE TO P-CSCF DIRECTION))
S803
IP SEC NECESSARY / UNNECESSARY ACKNOWLEDGEMENT REQUEST (IP ADDRESS)
S804
COMPARE IP ADDRESS AND IP ADDRESS LIST
S805
COMPARE OPERATOR IDENTIFIER
S806
RESPONSE (IP SEC IS UNNECESSARY)
S807
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S808
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S809
STORES SECRET KEY, INTEGRITY KEY
S810
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC ARE UNNECESSARY)
S811
SIP REGISTRATION (RESPONSE TO UNNECESSARY USER ID, CHALLENGE RESPONSE, AND IP SEC)
S812
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S813
AUTHENTICATION OK
S814
AUTHENTICATION OK
S815

FIG. 20

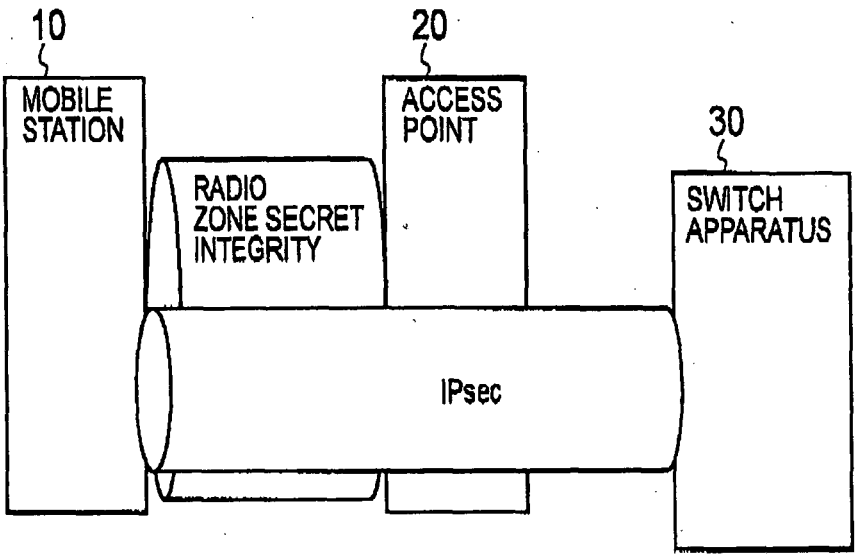
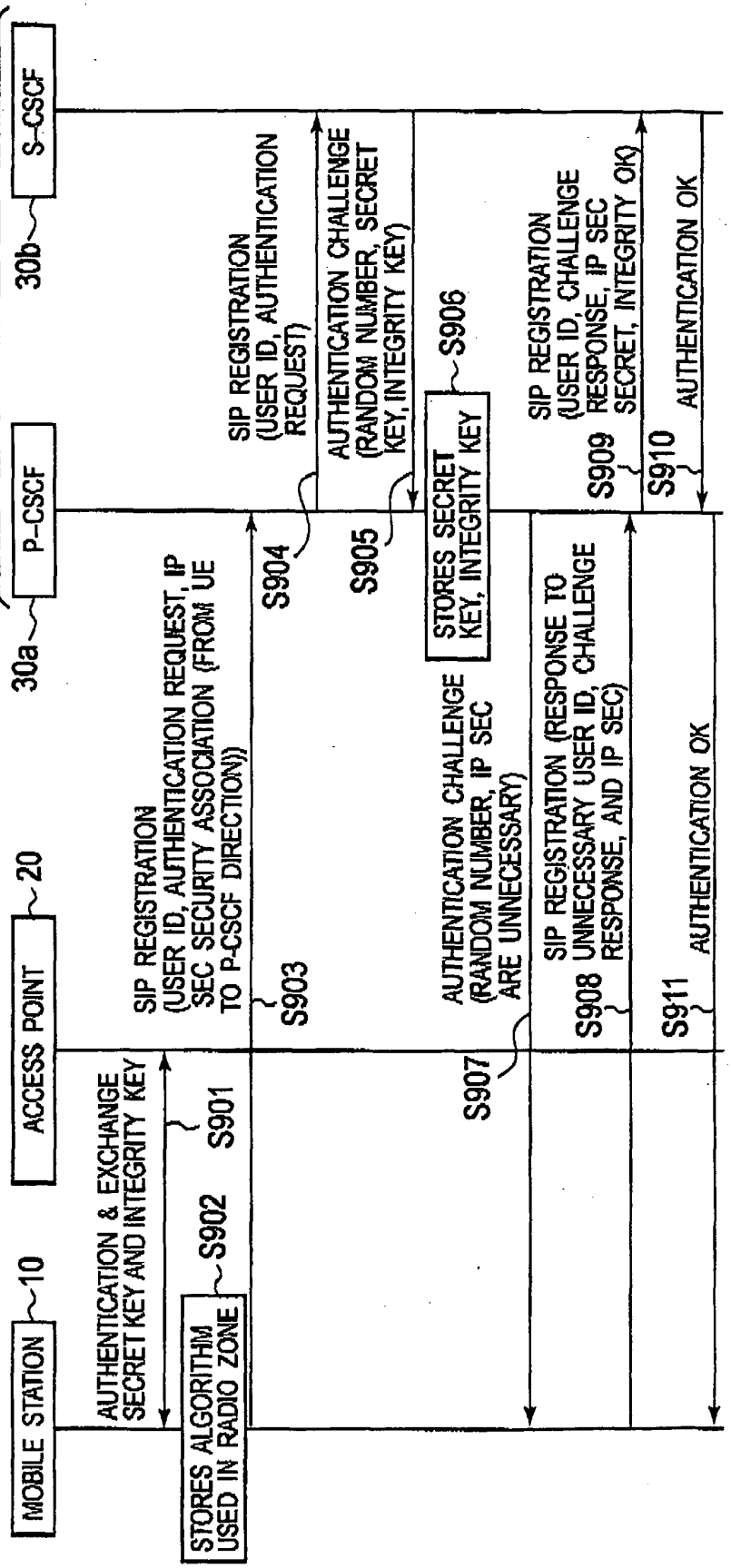

10
MOBILE STATION
20
ACCESS POINT
30
SWITCH APPARATUS
RADIO ZONE SECRET INTEGRITY
IPsec

FIG. 21


30 SWITCH APPARATUS
MOBILE STATION
10
ACCESS POINT
20
30a
P-CSCF
30b
S-CSCF
AUTHENTICATION & EXCHANGE SECRET KEY AND INTEGRITY KEY
S901
STORES ALGORITHM USED IN RADIO ZONE
S902
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST, IP SEC SECURITY ASSOCIATION (FROM UE TO P-CSCF DIRECTION))
S903
SIP REGISTRATION (USER ID, AUTHENTICATION REQUEST)
S904
AUTHENTICATION CHALLENGE (RANDOM NUMBER, SECRET KEY, INTEGRITY KEY)
S905
STORES SECRET KEY, INTEGRITY KEY
S906
AUTHENTICATION CHALLENGE (RANDOM NUMBER, IP SEC ARE UNNECESSARY)
S907
SIP REGISTRATION (RESPONSE TO UNNECESSARY USER ID, CHALLENGE RESPONSE, AND IP SEC)
S908
SIP REGISTRATION (USER ID, CHALLENGE RESPONSE, IP SEC SECRET, INTEGRITY OK)
S909
AUTHENTICATION OK
S910
AUTHENTICATION OK
S911

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/321893

A. CLASSIFICATION OF SUBJECT MATTER
H04L12/56(2006.01)i, *H04L9/32*(2006.01)i, *H04L12/22*(2006.01)i, *H04M3/00*(2006.01)i, *H04Q7/38*(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L12/56, H04L9/32, H04L12/22, H04M3/00, H04Q7/38

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2006
Kokai Jitsuyo Shinan Koho	1971-2006	Toroku Jitsuyo Shinan Koho	1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2005-510949 A (Telefonaktiebolaget L.M. Ericsson (publ)), 21 April, 2005 (21.04.05), Par. Nos. [0015], [0021], [0022]; all drawings & US 2003/0100291 A1 & WO 2003/047154 A1 & EP 1451963 A1	1,10,12 2-9,11
Y A	3GPP TS 33.203 V6.8.0 [online],2005.09. [retrieved on 2006.11.16],Retrieved from the Internet:<http://www.3gpp.org/ftp/Specs/archive/33_series/33.203/>	1,10,12 2-9,11
A	JP 2004-528761 A (Bluesocket Inc.), 16 September, 2004 (16.09.04), Full text; all drawings & US 2002/0136226 A1 & WO 2002/077820 A1 & EP 1381950 A1	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 November, 2006 (17.11.06)	28 November, 2006 (28.11.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (April 2005)